me net
curity
ide

NetworkLife

page 18.

NetworkWorld

The leader in network knowledge ■ www.nwfusion.com

March 28, 2005 ■ Volume 22, Number 12

A Wider Net

Yet another foolish

$20B federal

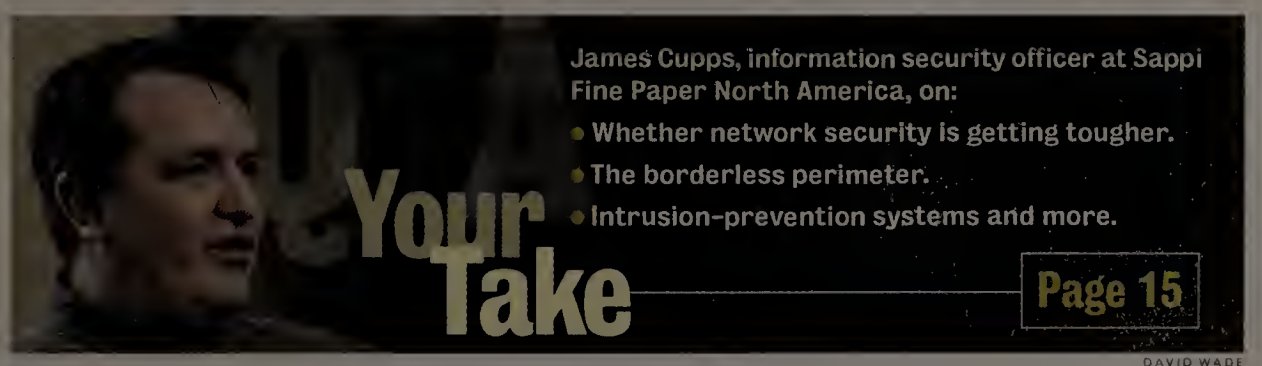
...ber of organizations have come forward in the past month or so to acknowl-

...national conference of industry and law enforcement to talk openly about this and what tools are

See Identity theft, page 14

DAN VASCONCELLOS

NEWSPAPER ■ $5.00



DAVID WADE

NetworkWorld® LIVE 05
TECHNOLOGY TOUR AND EXPO

THIS EVENT IS COMING TO A CITY NEAR YOU

DALLAS, TX | April 5, 2005 SAN FRANCISCO, CA | April 7, 2005
WASHINGTON, DC | April 12, 2005 NEW YORK, NY | April 14, 2005

Remote Office Networking:

Bringing the Enterprise Together

Remote Office Networking shows you how to satisfy your enterprise's seemingly conflicting demands for remote office networking without sacrificing control; flexibility as well as protection from hackers; more user productivity while lowering costs for supporting far-flung workgroups.

At **Remote Office Networking**, you'll get immediate-impact ideas, information and options that will reduce your remote office costs, increase your core security, and maximize your management efficiency. All while building an integrated remote office network that unites your enterprise.

Register now at www.nwfusion.com/RONS5WR2
or call Dori Smith at 800-643-4668

COMPLIMENTARY EVENT FOR PROFESSIONALS ONLY

GAIN TOOLS AND SERVICES TO HELP YOU:

- Build firewalls for the most open networks
- Secure users no matter where they're accessing from
- Evaluate which is for you, hardware VPNs or software VPNs
- Improve core-quality protection with authentication and authorization systems
- Deploy remote-centric backup and disaster recovery plans
- Create reliable voice and data connections, even via VoIP
- Provide productivity-boasting communications services to mobile workers
- Forecast and control collaboration and team project costs

WHO WILL BE THERE?

- Join James Gaskin, Principal, Gaskin Computer Services and Member of Network World Lab Alliance
- IT professionals with authority over remote office implementation, including:
  - CIOs
  - VPs/Directors of Networking
  - Network Managers
  - Business Line Managers
- Leading solutions partners

PRESENTING SPONSORS

3com Exercise Choice™
ADTRAN
INTERNET|SECURITY|SYSTEMS® Ahead of the threat.
RIVERBED

EXHIBITING SPONSORS

cyclades
IKlogix A WEBSENSE PARTNER
netopia
Raritan. When you're ready to take control.™
softwaremedium A WEBSENSE PARTNER
TelePacific COMMUNICATIONS

This event is limited to Network and IT professionals involved in the evaluation, purchase and implementation of network products and services. Network World Events reserves the right to determine total audience and profile of complimentary attendees. Paid registration is also available.

me net
curity
de

NetworkLife

page 18.

NetworkWorld

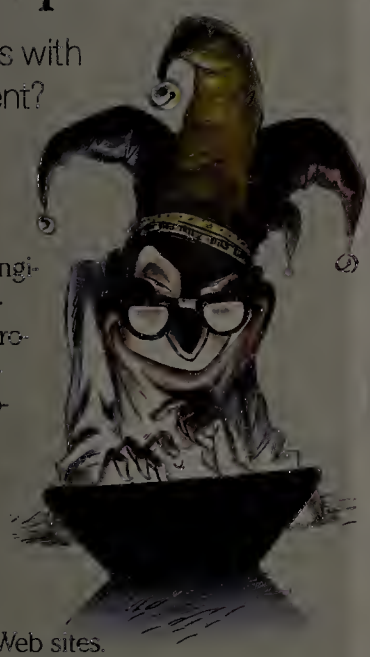
The leader in network knowledge ■ www.nwfusion.com

March 28, 2005 ■ Volume 22, Number 12

A Wider Net

Yet another foolish network protocol

IETF in cahoots with law enforcement?



■ BY CAROLYN DUFFY MARSAN

The Internet engineering community has proposed a new communications protocol designed to help prosecutors track down people who illegally download copyrighted material from peer-to-peer Web sites.

The so-called Omniscience Protocol would be installed on all Internet-enabled devices that can be used to play protected material, including computers and MP3 players.

The protocol will work even when a user's Internet connection fails. "Since the evil-doer might try to hide his or her evil-doing by disconnecting the computer from the network, the Omniscience Protocol must be able to continue to communicate even under these circumstances," writes protocol author Scott Bradner, a senior technical consultant at Harvard University.

Gotcha!

This April Fool's joke was published last year by the Internet engineering community.

See April Fool's, page 64

DAN VASCONCELLOS

$20B federal contract has telcos salivating

■ BY CAROLYN DUFFY MARSAN

The U.S. government is expected to release in April an RFP for a 10-year, $20 billion telecom services buy that is thought to be the largest pending network deal in the world.

The so-called Networx program will provide legacy and leading-edge voice, data and video services to all U.S. federal agencies. Every major U.S. telecom carrier — AT&T, MCI, SBC, Sprint, Qwest and Verizon — is expected to bid on it.

Networx is so huge and so important to the overall financial health of U.S. carriers that it is attracting an unprecedented level of interest from telecom industry executives, CEOs and directors.

"If you accept that it's worth $20 billion, Networx is the largest deal that's out there right now," says Jim Payne, senior vice president and general manager of Qwest Government Services Division. "Even if you look at it conservatively and say it's worth $3 billion or $4 billion, it's still the largest deal."

Payne says the Networx bid is getting "a lot of attention" from Qwest's corporate headquarters. "They have reviewed Networx at the senior executive level a half-dozen times, and we are regularly briefing them on it," he says.

Networx is "a very, very high priority within AT&T," says Bob

See Networx, page 12

High-profile identify thefts force govt., industry to take action

■ BY ELLEN MESSMER

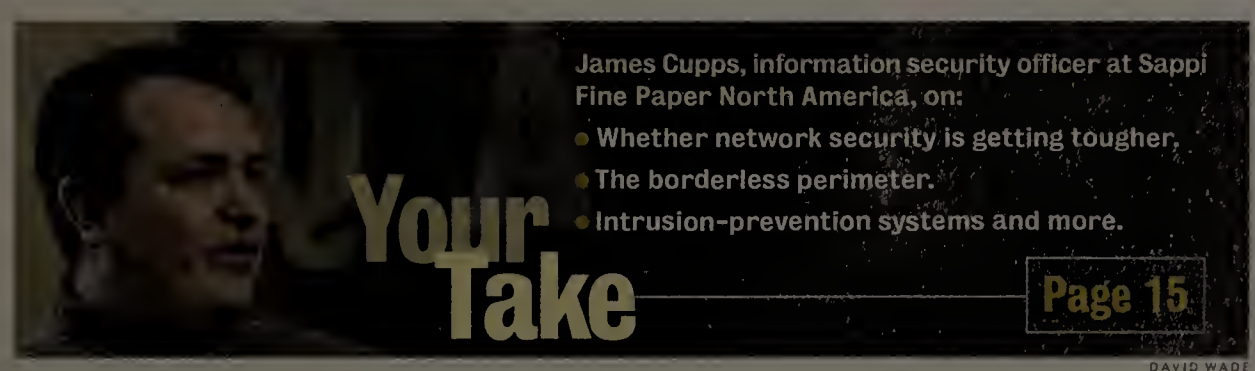
The recent rash of identity thefts has businesses and government agencies exploring new options for locking down resources and setting policies to prevent easy pilfering.

The problem — the Federal Trade Commission logged 635,000 consumer complaints for fraud and identity theft last year, with 61% for fraud and 39% for identity theft — is reaching critical mass. A growing number of organizations have come forward in the past month or so to acknowledge massive theft of the personal data they hold. SAIC, Bank of America, George Mason University, Boston College, Retail Ventures, the Las Vegas Department of Motor Vehicles and LexisNexis all confessed to security breaches, both high- and low-tech. ChoicePoint, after admitting it unwittingly sold personal data to those involved in identity theft, triggered public outrage and a Capitol Hill inquiry.

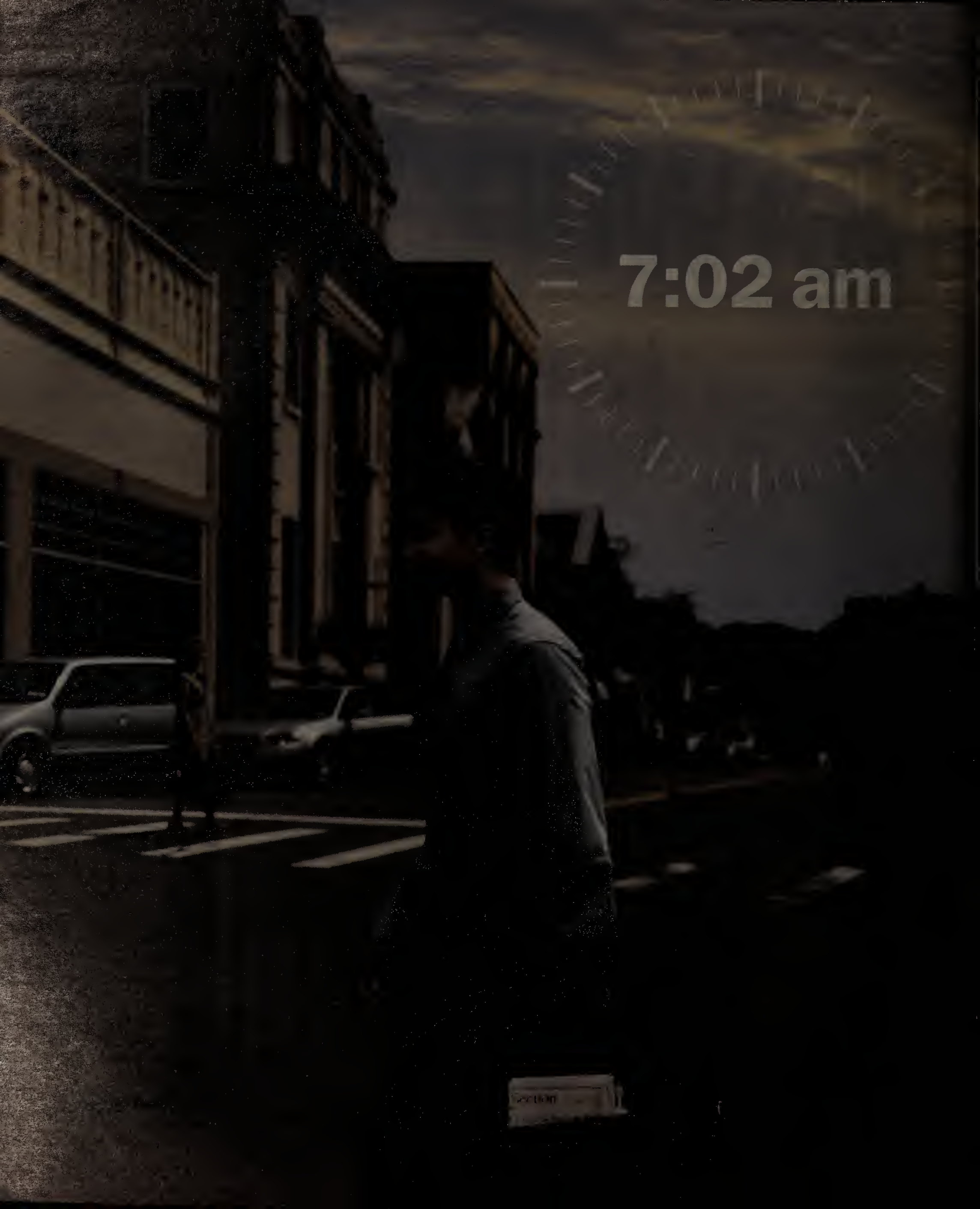
"We need to convene a national conference of industry and law enforcement to talk openly about this and what tools are

See Identity theft, page 14

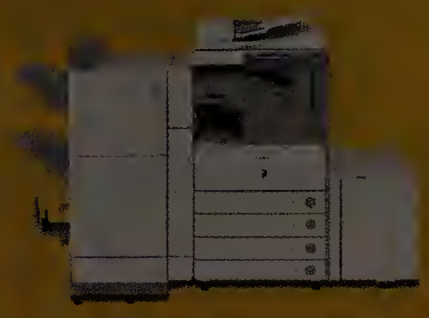
NEWSPAPER ■ $5.00



DAVID WADE


7:02 am

imageANYWARE™



imageRUNNER 4570

We brought the power of the network to the copier.

And the potential of another day is realized.

If you could create, manage, and share documents on paper or over the network, imagine what you could accomplish with your day. With Canon's latest addition to the imageRUNNER line, every day's potential can be realized. With the new imageRUNNER 4570, Canon gives you another innovative solution to seamlessly integrate the paper world with the digital world. And the imageRUNNER 4570 can be tailored to meet your business needs. In other words, when you choose the new imageRUNNER 4570, you choose to work the way you need to.

www.imagerunner.com 1-800-OK-CANON

Not business as usual.

Canon KNOW HOW®

Sam, don't lock them in. Get on Solaris™ 10!

What would you do with a 10,000 CPU grid?

Pay $1 to find out.

Introducing the *Sun Grid* for $1/cpu-hr. The network is your computer.

If you're paying more than $1/cpu-hr to build and run your own grid, you're overpaying. Because that's the price at which our grid is available to you. Pay $1/cpu-hr, and leverage our capital spend, SPARC® or x86 computers, storage, and facilities to run your business. From Monte Carlo simulations to reservoir simulation. Protein modeling to movie rendering. 1 cpu to as many as you could conceive. No minimum commitment, no maximum. Stretch your dollar at sun.com/sungrid

Sun microsystems
The Network is the Computer™

solaris Java

Network News

Net Infrastructure

Enterprise Computing

Application Services

The Verizon 620 helps your road warriors connect from afar. Page 40.

Service Providers

Technology Update

Opinions

Management Strategies

■ **CONTACT US** Network World, 118 Turnpike Road, Southborough, MA 01772; **Phone:** (508) 460-3333; **Fax:** (508) 490-6438; **E-mail:** nwnews@ nww.com; **STAFF:** See the masthead on page 14 for more contact information. **REPRINTS:** (717) 399-1900

SUBSCRIPTIONS/CHANGE OF ADDRESS: Phone: (508) 490-6444; Fax: (508) 490-6400; E-mail: nwcirc@nww.com; URL: www.subscribenw.com

28/05

VoIP special report:

CLEAR CHOICE TEST

More online

NetworkLife

The expert's guide to the connected home

page 18.

Online: www.nwfusion.com

Breaking News

Go online for breaking news every day. **DocFinder: 6342**

Available only on Fusion

Last call: Network World Renovator Award

Have you overhauled your network and realized a substantial return on the investment, discovered a significant new business opportunity or found a creative way to leverage technology? If so, get in the running for *Network World's* new Renovator Award. The deadline for entries is Monday, April 4. **DocFinder: 6093**

Network World Radio: Linux in the data center

NW Radio headed to IDC's Directions 2005 conference to talk with Jean Bozman, research vice president for the enterprise computing group, about Linux in the data center. We also talked to Kevin Burden, program manager for mobile devices, about the future of the phones and PDAs we carry. **DocFinder: 6450**

Network Life: Spotlight on home network security

Keeping home nets free from viruses, bugs, spyware and worms isn't easy. The latest edition of *Network Life* offers strategies on securing your home network; 10 ways to stop spyware; tests of a WLAN security system and a WLAN extender; and much more. **DocFinder: 6451**

A Wider Net

If you've missed any of our weekly stories that go beyond the speeds and feeds of the network and IT industries — like a look at the nation's elite science and technology high school or stories of married net pros — check out the Wider Net archive. **DocFinder: 6452**

Free e-mail newsletters

Sign up for any of more than 50 newsletters on key network topics. **DocFinder: 6343**

What is DocFinder?

We've made it easy to access articles and resources online. Simply enter the four-digit DocFinder number in the search box on the home page, and you'll jump directly to the requested information.

Online help and advice

Nutter's Help Desk

Sniffing VoIP

Help Desk guru Ron Nutter helps a reader who asks: "When our current PBX goes off maintenance, we'll look at making the change to a newer system, probably one based on VoIP. Since how well the system works will depend on how well the network is running, what type of tools should I have to be able to properly tell what's going on?" **DocFinder: 6453**

Gearblog

Daddy, where do MP3s come from?

Columnist Mark Gibbs examines StationRipper and StreamRipper, which let you build a music library by tuning into Internet radio stations and saving their streams to disk. **DocFinder: 6454**

Telework Beat

Future of Work Congress sneak peek

Net.Worker Managing Editor Toni Kistner says those who attend the upcoming Future of Work Congress can expect less pie in the sky, more takeaway. **DocFinder: 6455**

Home Base

Managing your books and contacts, Part 2

Columnist Sandra Gittlen finds that QuickBooks Premier Edition suits a growing business. **DocFinder: 6456**

Small-Business Tech

Getting out from under Outlook, Part 2

Columnist James Gaskin advises that you clean out your in-box and then test drive one of the Microsoft-free e-mail clients he suggests. **DocFinder: 6457**

Seminars and Events

Remote-Office Networking: Bringing the Enterprise Together

A new Technology Tour Event and Expo packed with immediate-impact ideas, information and options that will reduce your remote office costs, increase your core security and maximize your management efficiency. Find out how you can qualify to attend free. **DocFinder: 6458**

News Bits

Supreme Court to rule on sharing

■ The U.S. Supreme Court this week hears arguments for forcing cable TV operators to share their lines with other service providers, much the same way that phone companies are required to lease phone lines to their competitors. Currently, the FCC says cable companies don't have to share, but a federal appeals judge has ruled that they must. If the Supreme Court rules against sharing, broadband ISPs that don't own wires to customers' homes will have one less option for hooking them up. The FCC argues that cable TV lines should not be subject to open-access rules that govern voice networks because cable TV is a data service, not a voice service — although voice services can run over the same lines. Supreme Court decisions typically take months.

Mobility madness

■ Just before Cisco closed its $450 million acquisition of Airespace last week, competitors Nortel and Alcatel, which previously resold Airespace gear, announced new wireless LAN partners. Nortel said it will resell WLAN switching gear from Trapeze Networks. The new Nortel WLAN switch line will be called the Nortel WLAN 2300 — based on Trapeze's MX products — and will ship by midyear. Nortel also said it will continue to support the Airespace-based gear it has sold since March 2003. Meanwhile, Alcatel last week partnered with Trapeze rival Aruba Wireless Networks to fill its WLAN technology gap. Alcatel will integrate Aruba's WLAN switching and access point technology into its CrystalSec architecture for LAN and WLAN security and mobility.

IT budgets get some growth hormone

■ IT budgets will increase by 4.6% in 2005 and by 5.3% in 2006, according to an SG Cowen Technology Research Team study released last week. The firm reports the 2005 projection is up from 3.7% in its December survey. "While the overall pace of growth remains modest, several of the key metrics we track, including IT budget growth, IT capacity demand and IT project priorities, edged back up from the softer results in our December survey," the firm said in a statement. February's survey of more than 215 North American IT users shows 70% of respondents expect their business to improve over the next 12 months. Researchers credit Sarbanes-Oxley regulatory requirements with increasing budgets in the first half of 2005, saying it's "more of a boost than a hindrance to spending." Spending priorities also remained high for security, disaster recovery and internal development, and improved most for storage-area networks, storage consolidation and CRM. Lastly, the group found the PC upgrade cycle eased a bit in favor of servers and storage.

BMC buys more identity

■ BMC Software last week continued its identity management quest by announcing it would buy OpenNetwork Technologies, a maker of Web access management and single sign-on technology, for $18 million. The acquisition of privately held OpenNetwork will add technology for securely managing federated user identities and Web-based applications to BMC's identity management product suite. The news comes just two months after BMC said it would purchase Calendra and its identity management technology.

Everybody settle up

■ IBM has reached a settlement with software developer Compuware, which sued IBM in 2002 for a litany of alleged violations, including copyright infringement, antitrust law abuses and unfair competitive acts. Under the deal's terms, IBM will spend $400 million during the next four years on Compuware software and services, the two companies announced last week. IBM and Compuware also entered a patent cross-licensing agreement and will exchange technical information to ensure interoperability of their products. Compuware's product portfolio includes management software for IBM's mainframes. Meanwhile, Quest Software has agreed to pay $16 million plus additional royalties to Computer Associates to settle a lawsuit CA filed in 2002 accusing Quest of illegally using CA source code. Last week's deal also resolves Quest counterclaims that challenge the validity of some CA copyrights. Under the settlement's terms, neither Quest nor CA admitted wrongdoing.

Europe gets its .eu

■ There is new hope for those waiting for the domain name suffix ".eu" to be brought to life, in what already has been a seven-and-a-half-year process. The Internet Corporation for Assigned Names and Numbers, the body that oversees technical matters related to the Internet, last week approved the application from the European Registry of Internet Domain names to take the new Top Level Domain into ICANN's root files. EURid was chosen by the European Union's executive body, the European Commission, to manage the .eu TLD. The nonprofit group has long contended that the creation of the .eu TLD is an important step in promoting e-commerce in Europe and the European identity, and for creating higher visibility of the internal market.

TheGoodTheBadTheUgly

JavaOne: Where the shirts hit the fans. Among the highlights at this June's JavaOne Conference in San Francisco? A contest for building a system to hurl souvenir T-shirts into the audience during general sessions (https://tshc.dev.java.net/). ▼

Patching Firefox. The Mozilla Foundation is getting a little taste of what Microsoft goes through. The nonprofit open source group last week issued its second security patch in a month to protect users of its Firefox Web browser.

Vonage slapped with lawsuit. Texas Attorney General Greg Abbott filed a lawsuit last week against Vonage accusing the fast-growing VoIP provider of not warning customers about limits to its 911 emergency dialing service. A company spokeswoman said Vonage would welcome a dialog with Abbott on how to improve its 911 service.

RECLAIM YOUR EMAIL

Visit us at Info Sec.
Booth #813
Orlando

Spam and virus protection at an affordable price.

- No per user license fees
- Prices starting at $1399
- Powerful, enterprise-class solution

Barracuda Spam Firewall

BARRACUDA NETWORKS

Order a free evaluation unit at
www.barracudanetworks.com

POWERFUL EASY TO USE AFFORDABLE

Aggressive Reseller Program
Get more info by visiting www.barracudanetworks.com/ifo
or by calling 1-888-ANTI-SPAM or 408-342-5400

BrainShare shift: Netware to Linux

■ BY DENI CONNOR

SALT LAKE CITY — For the past few years Novell has been talking up Linux and downplaying NetWare. At the company's annual BrainShare conference last week, even die-hard NetWare customers started to do the same.

"Our [IT] director has said that he wants every system in our network to go to Linux," said Dan Tesenair, senior network engineer at Health First in Melbourne, Fla. The healthcare provider is moving Windows, Unix and NetWare servers to a mix of Novell's SuSE Linux and Open Enterprise Server (OES), which is based on Linux and NetWare kernels.

Novell last week tried to give customers even more reason to buy into its open-source-oriented strategy, which is designed to meld the best of Linux and NetWare services. The company announced that its GroupWise messaging and collaboration system will come bundled with SuSE Linux, and its ZENworks systems management offering will be able to control Windows workstations from Linux servers.

Novell also introduced a Linux-based network and collaboration package for small and midsize businesses that will be available through partners such as Dell and HP. What's more, the company said it formed the Open Source Technology Center, which will promote development of open source and Linux applications.

Announcements like those are aimed squarely at IT professionals such as Roger Fenner, who was among the 4,000 users and Novell partners attending BrainShare at the Salt Lake Convention Center. Fenner is infrastructure services manager for Comair, a subsidiary of Delta Airlines, in Cincinnati.

Comair is making the move to OES, rolling out Intel Itanium-based HP Integrity servers running SuSE Linux in place of PA-RISC machines running HP-UX.

"Sixty-four-bit computing on Itanium servers is a big part of our hardware infrastructure plans," he said. "SuSE Linux is very much invested in the 64-bit architecture."

Fenner also is moving from Windows and NetWare on ProLiant servers to OES, which supports file and print, ZENworks, NetMail, GroupWise and other NetWare services on the SuSE kernel.

"With HP-UX [on PA-RISC] going away, it will be nice to have a common platform for everything," said Fenner, who has 55 PA-RISC servers and 55 ProLiants.

His BorderManager and iChain applications will remain on OES running the NetWare kernel, although Fenner said the recently introduced Novell Security Manager, an OEM product from Astaro that runs on Linux, excites him. ■

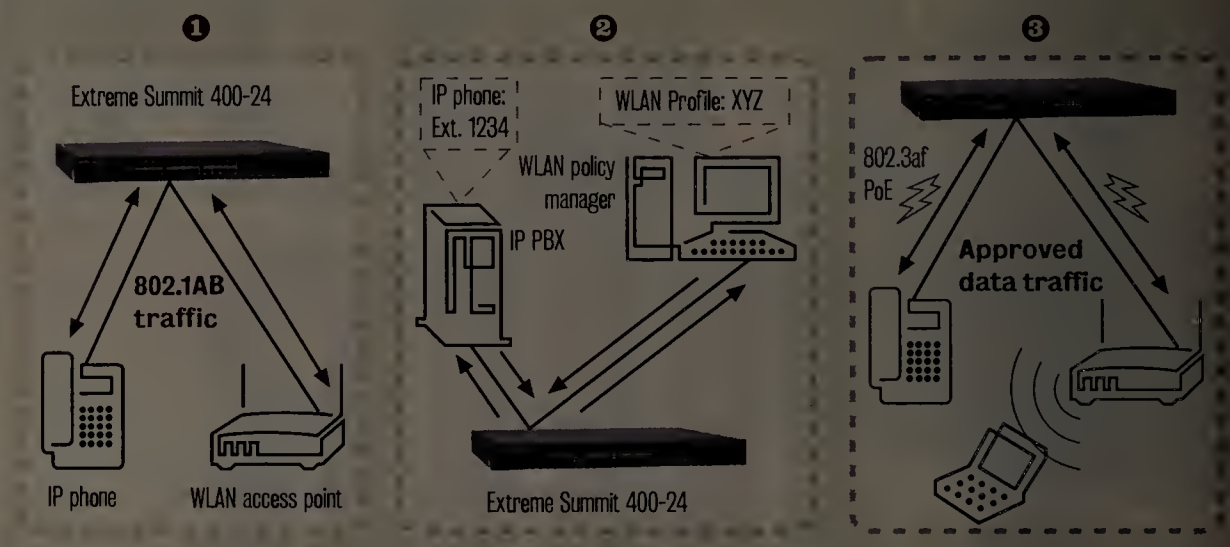
It's showtime

A sampling of Novell's BrainShare announcements.

Product or technology	Function
GroupWise support for ten years	Provides notice to users that GroupWise is not dead.
Linux Small Business Suite	Network and collaboration tools on Linux for SMBs.
Acquired Tally Systems	Adds inventory, auditing and compliance to its ZENworks package.
Open Source Technology Center	Promotes development of open source applications
Validated Configuration Program for Data Center	Certifies multi-application stacks on Linux.
ZENworks 7 Suite	Allows Windows desktop management from Linux servers.

Plug and play

Extreme's Summit 400-24 switch lets devices autoconfigure themselves on a LAN via Link Layer Discovery Protocol (802.1AB).



❶ An IP phone and WLAN access point register themselves with the switch via 802.1AB information.

❷ The Extreme switch relays 802.1AB data to back-end devices for authentication and configuration data.

❸ The switch delivers configuration settings, applies profiles and runs Power over Ethernet to approved devices.

Extreme's new switch to hook up IP phones, Wi-Fi gear

■ BY PHIL HOCHMUTH

Extreme Networks this week is expected to launch a LAN edge switch designed to simplify deployments of wireless LAN access points and IP phones, using an emerging standard protocol for device discovery.

Extreme's Summit 400-24 combines features such as centralized WLAN switch management and configuration, and Power over Ethernet (PoE) and 802.1X technology to help streamline the deployment of secure WLAN and VoIP networks. The switch also uses the emerging Link Layer Discovery Protocol (802.1AB), which can let the switch discover and configure endpoints such as IP phones and Wi-Fi access points on the fly.

Music instrument retailer Guitar Center is in the middle of corporate-wide deployment of Extreme's previously released 48-port version of the Summit 400. The switches will support Extreme WLAN access points the company is putting into its stores, around two per store in 150 locations nationwide.

"We depend a lot on wireless for inventory control," says Robert Hill, IS director for Guitar Center. He says the store uses bar-code reading guns from Symbol Technologies, which let data be uploaded to a central database via Wi-Fi.

The benefit of the Summit 400 series is its use of thin access points, Hill says. "This is where the industry is moving towards. I like the idea of having thin [access points] and switches all rolled up into a centrally managed console." This lets IS staff distribute wireless and LAN security rules from its Thousand Oaks, Calif., headquarters without having to touch hardware in the stores.

In the near future, Hill says, Guitar Center also might move its network of 3Com NBX IP PBXs — which support voice for all stores — onto the Extreme Summit 400 switches. However, those systems now run on recently bought 3Com SuperStacks, which are "working fine," he says.

The Summit 400-24 has 24 triple-speed Ethernet ports and four Gigabit uplinks (fiber or copper). Stacking ports on the back of the switch lets boxes be daisy-chained in a stack, with 20G bit/sec of bandwidth between switches.

The switch supports 802.1X authentication, which forces end users to authenticate at the port level. This provides greater security for wired or wireless end users. The Summit 400 also provides WLAN switching capabilities, such as support for thin access points, centralized access point management and fast-handoff support for roaming between access points on different subnets.

New to the Summit 400 box is the recently ratified IEEE 802.1AB standard. This technology is similar to Cisco's Discovery Protocol, widely used on all-Cisco-based LANs, where switches, routers and IP phones can discover each other over Ethernet.

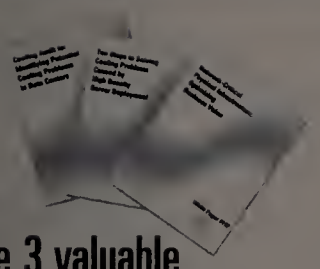
Gear supporting the 802.1AB standard will be able to store this data, as well. This lets a switch or other piece of equipment be "aware" of its neighbor. Having gear that learns such information as QoS parameters, PoE power settings and other configuration data from other gear could help reduce the amount of footwork required for large IP telephony rollouts.

Extreme plans to roll out support for 802.1AB for the rest of its switch line in the spring. Extreme says that its IP telephony partner Avaya will introduce 802.1AB support on its IP phones, IP PBXs and gateways later this year.

The Summit 400 competes with switches that combine wired and WLAN switching capabilities, including gear from Airespace (now Cisco), Aruba Networks, Foundry and Trapeze.

The Summit 400-24 will be available in April for $4,500. ■

■ Examine Force10's stackable offering for data centers. PAGE 17.



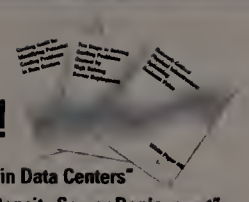
hoose
nd receive
ny of these 3 valuable
PC white papers within
e next 90 days for FREE!

tp://promo.apc.com **Key Code** y579y

38) 289-APCC x3349 • FAX: (401) 788-2792

APC
Legendary Reliability®

Choose and receive any of these 3 APC white papers within the next 90 days for FREE!



- ☐ White Paper #40 **"Cooling Audit for Identifying Potential Cooling Problems in Data Centers"**
- ☐ White Paper #42 **"Ten Steps to Solving Cooling Problems Caused by High Density Server Deployment"**
- ☐ White Paper #117 **"Network-Critical Physical Infrastructure: Optimizing Business Value"**

☐ **YES!** Please send me my FREE white papers. ☐ **NO,** I'm not interested at this time, but please add me to your mailing list.

Name: Title:

Company:

Address: Address 2:

City/Town: State: Zip: Country:

Phone: Fax: E-mail:

☐ ***Yes!*** ***Send me more information via e-mail and sign me up for APC PowerNews e-mail newsletter.*** **Key Code** y579y

What type of availability solution do you need?
☐ UPS: 0-16kVA (Single-phase) ☐ UPS: 10-80kVA (3-phase AC) ☐ UPS: 80+ kVA (3-phase AC) ☐ DC Power
☐ Network Enclosures and Racks ☐ Precision Air Conditioning ☐ Monitoring and Management
☐ Cables/Wires ☐ Mobile Protection ☐ Surge Protection ☐ UPS Upgrade ☐ Don't know
Purchase timeframe? ☐ < 1 Month ☐ 1-3 Months ☐ 3-12 Months ☐ 1 Yr. Plus ☐ Don't know
You are (check 1): ☐ Home/Home Office ☐ Business (<1000 employees) ☐ Large Corp. (>1000 employees)
☐ Gov't, Education, Public Org. ☐ APC Sellers & Partners

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 36 WEST KINGSTON RI

POSTAGE WILL BE PAID BY ADDRESSEE

APC

ATTENTION CRC: y579y
Department: B
132 FAIRGROUNDS ROAD
PO BOX 278
WEST KINGSTON RI 02892-9920

How to Contact APC

Call: (888) 289-APCC
use the extension on the reverse side

Fax: (401) 788-2792

Visit: *http://promo.apcc.com*
use the key code on the reverse side

APC
Legendary Reliability®

Introducing data centers on demand

New architecture supports power densities of today... and tomorrow

Hot-aisle Ceiling Tiles/Cable Trough
Seals in hot air, prevents mixing with room air

WINNER
2004 BEST OF INTEROP
NETWORLD · INTEROP

BLADE READY™

APC solutions that carry the "Blade-Ready" Logo are designed to handle the demanding network-critical physical infrastructure requirements of high-density blade server applications.

Chamber Doors
Access to hot aisle, locks for security

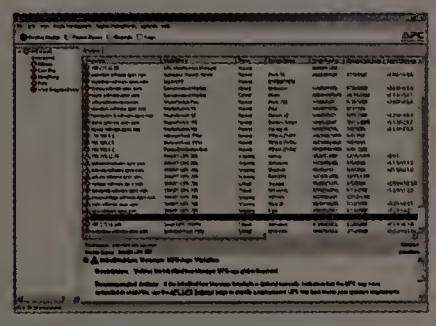
Now you can quickly deploy a standard- or high-density site of any size with scalable, top-tier availability.

Part Number	Usable IT Racks	Average kW per Rack	Price to buy	Price to lease (36 installments)
ISXCR1SY16K16P5	1	up to 5kW	$14,999*	$499**
ISXT240MD6R	6	up to 5kW	$149,999*	$4,999**
ISXT240MD11R	11	up to 5kW	$249,999*	$7,999**
ISXT280MD40R	40	up to 5kW	$699,999*	$21,999**
ISXT2800MD100R	100	up to 5kW	$1,649,999*	$50,999**
High Density Configuration *(shown above)*				
ISXT280HD8R	8	up to 10kW	$399,999*	$12,999**

High density upgrades start at $10,999
On-site power generation options start at $29,999

All multi-rack configurations feature:

- ✓ *N+1 power and cooling*
- ✓ *Secure, self-contained environment*
- ✓ *Peak capacity of 20kW per rack*
- ✓ *Enhanced service package*
- ✓ *Integrated management software*



InfraStruXure™ Manager

What is data center on demand?

InfraStruXure™

DATA CENTERS ON DEMAND

Highly available and manageable, quick-to-install, scalable architecture that easily supports both standard- and high-density applications.

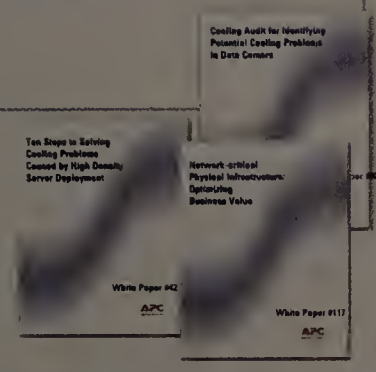
- *Up to 20kW a rack for any blade server application*
- *Unlimited racks*
- *Ships in 5 days****
- *Installs in 1 day****
- *Optional on-site power generation*
- *Raised floor not required*
- *Vendor neutral guaranteed compatibility*

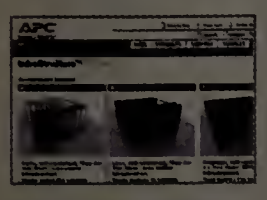
InfraStruXure™ can be purchased as a modular, conventional or mobile system

Order your solution today. Call 888-289-APCC x3349.

Visit today and receive FREE APC White Papers

Visit us online and download APC White Papers.





InfraStruXure™ BuildOut Tool

Don't see the configuration you need?

Try APC's online InfraStruXure™ BuildOut Tool today and build your own solution.

Go to *http://promo.apc.com* and enter key code y579y Call 888-289-APCC x3349

* Prices do not include IT equipment and are subject to change. ** Indicative rates are subject to market conditions. *** Install and delivery times may vary.

APC®
Legendary Reliability®

 E-mail: esupport@apcc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA ISX4D4EF-USc

Microsoft builds toward mgmt. vision

Updated software will add common features across patch and assessment tools.

■ BY JOHN FONTANA

After nearly two years, Microsoft last week began to pull together the first pieces of its patch management infrastructure. The effort ultimately will extend to a host of free and licensed products and eventually integrate with efforts to create a broad management platform for Windows.

The goal of the plan, which the vendor calls its Dynamic Systems Initiative (DSI), is to provide corporate users with a range of assessment, configuration, monitoring, management and development tools that will let Microsoft's software communicate its status to the network to improve the security, uptime and general maintenance of Microsoft environments.

In its march to that goal, Microsoft last week issued a final beta and a first beta for two technologies that will provide common scanning and catalog engines for future free and licensed patch and assessment tools. And next month at its annual management conference, Microsoft will issue a technology beta of its new capacity-planning tool, code-named Indy, to fill in more of its management puzzle.

"Microsoft's management is all about making Microsoft infrastructure as intelligent as possible in terms of managing itself," says Jasmine Noel, a principal with Ptak, Noel & Associates. "But you can't manage something if you don't know its configuration, and you need to be able to do that quickly and efficiently. They can't go to Step 2, which are things like capacity planning, until they solve Step 1, which is configuration."

Last week, Step 1 involved issuing the "release candidate" for its Windows Server Update Services (WSUS), a free server that corporations internally deploy to download patches from Microsoft and push them out to desktops and servers. A release candidate is the final step in the beta process before product shipment. Microsoft called the software Windows Update Services in the past. More than 100,000 copies of the 1.0 version, which is called Software Update Services, connect to Microsoft on a monthly basis to download patches.

The company also launched the beta program for Microsoft Update, a public Web-based patch download site and the replacement for the current Windows Update. Microsoft Update eventually will provide patches for all Microsoft software and will work in conjunction with WSUS.

"The significant things we have focused on is 'can we reduce the downtime and the costs associated with getting patches out to systems and getting them updated?'" says Felicity McGourty, director of product marketing in the Windows and enterprise management group at Microsoft. "The second thing we are focused on is 'can we reduce the costs as far as the labor?' The third aspect that we covered is to reduce data loss."

But Microsoft's goal is DSI, and WSUS and Microsoft Update form the foundation for all patch and assessment tools going forward. The linchpin is WSUS' new client-side scanning engine that details what patches are installed and catalog technology that lists available patches and updates.

Those two technologies eventually will replace similar features in Systems Management Server and Microsoft Operations Manager and will be part of the forthcoming System Center which will include the Indy capacity-planning tool.

Originally, Indy was slated for release with Longhorn in 2006 to 2007, but Microsoft now plans to release it sooner to enhance its management offerings.

WSUS, which only runs on Windows 2000 and 2003 servers and XP clients, is slated to ship before July 1, with Microsoft Update scheduled later in 2005, according to Microsoft officials. Initially, WSUS will support patches for Win 2000, Win 2003, XP, Office XP, Office 2003, SQL Server 2000, MSDE 2000 and Exchange 2003. ■

The art of the patch

Microsoft is gearing up to release the first technologies for its revamped portfolio of patch management software. One key is Windows Server Updates Services, which includes features that will be added to System Management Server 2003 and Microsoft Baseline Security Analyzer 2.0.

Product	Description	Availability, cost
Windows Server Update Services	[illegible]	[illegible]
Microsoft Update	Patch download site maintained by Microsoft.	Before year-end; free
System Management Server 2003	[illegible]	[illegible]
Microsoft Baseline Security Analyzer	Security assessment tool will incorporate WSUS scanning technology.	2.0 version available 30 days after WSUS; free

IBM, Symantec takes on spammers

■ BY CARA GARRETSON

Fighting spam is becoming as complex as ordering an eight-course meal off an a la carte menu, as vendors come up with new combinations of methods and a variety of form factors to help companies keep unwanted messages off their networks.

IBM is the latest vendor to jump into the anti-spam fray with a cocktail approach, layering a number of spam-fighting techniques to achieve maximum effectiveness. The company last week unveiled its Fair use of Unsolicited Commercial E-mail (FairUCE) technology that aims primarily to identify spam sources at the network level, eschewing content filtering altogether. IBM is making FairUCE freely available to members of its alphaWorks online community of developers and early adopters, and is assessing how to license the technology.

FairUCE, which is implemented as an SMTP proxy, weeds out spoofed e-mail sent from spammers, phishers and zombie PCs by using cached DNS look ups to match IP addresses with domain names, says Amit Patel, emerging technology strategist with IBM alphaWorks. If the IP address doesn't match the domain, FairUCE bounces the e-mail back to the sender with a challenge that they identify who they are, which won't be answered because the e-mail was unwanted to begin with, Patel says.

This approach is similar to challenge response software, except with that model every piece of incoming mail is challenged under the assumption that valid senders will verify their identity. FairUCE only challenges messages where the domain and the IP address don't match, Patel says. It also includes a whitelist so users can denote senders who should never be challenged.

It's not so much that FairUCE is groundbreaking technology, but that IBM is validating the sender domain identity verification approach that makes the announcement important, says Steven O'Grady, a senior analyst at Redmonk. "It's not really rocket science, but that IBM is putting something like this together and saying 'spam is a problem that's worth solving.'"

Because the majority of spam comes from spoofed e-mail sources, this identity-verification method catches 95% to 98% of unwanted messages, Patel says. In the instances where spammers use their legitimate e-mail addresses, FairUCE offers a blacklist for denoting IP addresses from which e-mail should never be received and a reputation service that collects historical data regarding an IP address' sending habits to help administrators determine whether the address is a source of spam.

Symantec also announced the third component of its e-mail security strategy, a hosting service that filters spam and viruses and controls compliance for companies.

Symantec Hosted Mail Security, priced starting at $1,710 per year for 50 users, complements the company's gateway software and gateway appliance. All three options provide the same virus protection, spam filtering and enforcement of corporate and regulatory compliance, which lets each company decide which approach is the best fit, says Chris Miller, group product manager with Symantec.

E-mail security maker Proofpoint this week will join Symantec in offering its messaging product in three different form factors. The company, which already sells its Proofpoint Protection Server gateway software and Proofpoint Messaging Security Gateway appliance directly to companies, is making both available as a hosted service via partnering managed service providers, according to company officials. ■

Lovely spam

One in every

1.3

e-mails sent in February was spam, and 1 in every 46.1 e-mails contained a virus, Trojan or other malicious content.

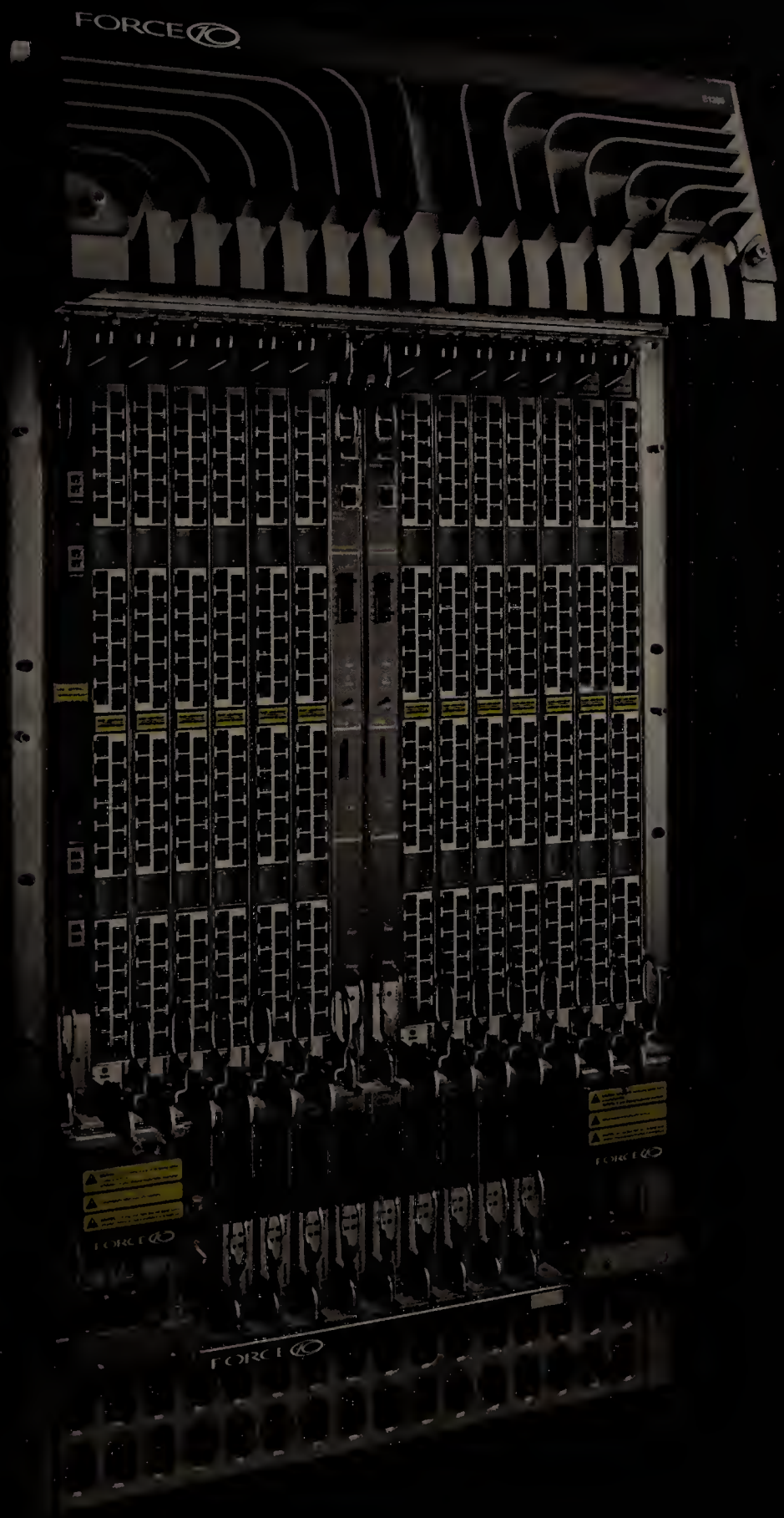
SOURCE: IBM'S GLOBAL BUSINESS SECURITY INDEX REPORT FOR FEBRUARY 2005

Fastest Throughput

Most Secure

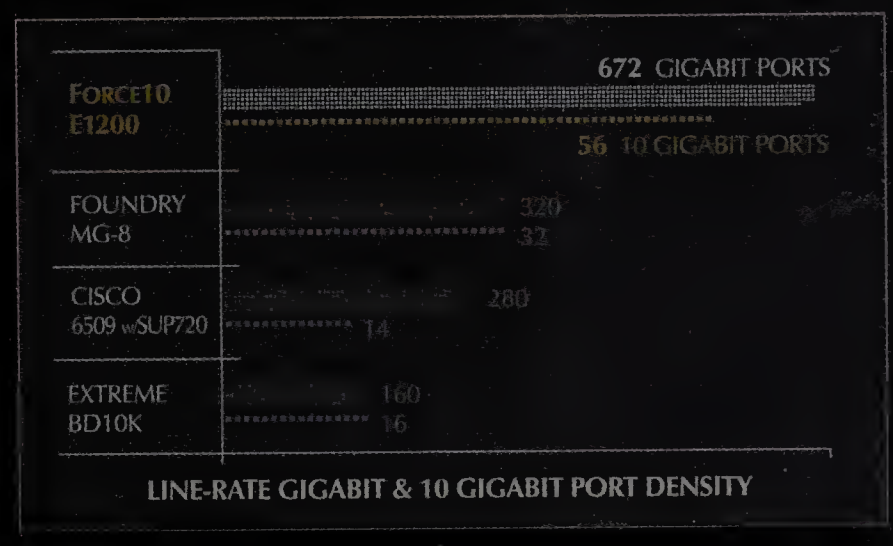
Highest Density

Greatest Resiliency



Were this a fine German car,
you would ask for a test drive.

We offer this simple chart.



You admire precision engineering and seek out maximum performance. You want the best. Presenting the E-Series from Force10 Networks: The first resilient switch/router to deliver 672 line-rate Gigabit Ethernet or 56 line-rate 10 Gigabit Ethernet ports per chassis — more than twice the capacity of our competitors. That's Terabit performance.

Based on Force10's revolutionary TeraScale™ technology, the E-Series delivers industry-best metrics in density, throughput, resiliency and security. The advanced architecture of the E-Series ensures predictable performance with traffic-variation dampening, provides control plane resiliency to prevent DoS attacks, and supports line-rate, real-time security filters for high performance security.

To test drive the E-Series in your network, contact us at 1-866-600-5100 or visit www.force10networks.com.

FORCE10™

To view independent TeraScale test results from The Tolly Group, visit www.force10networks.com

Dell touts database servers

■ BY JENNIFER MEARS

Dell last week expanded its high-end server options with the introduction of two new four-way servers designed to support powerful database applications.

The Dell PowerEdge 6800 and PowerEdge 6850 are based on Intel's newest 32-/64-bit Xeon processor, which Intel will unveil formally on Tuesday. Intel rolled out its 32-/64-bit Xeon for dual-processor servers last year, but this is the initial release of the hybrid chip for multiprocessor servers.

Enterprise users also can expect systems based on the chip from HP and IBM.

Dell executives say the PowerEdge 6800 and 6850 — which start at just under $4,000 and just under $5,000, respectively — are the lowest-priced four-way servers the computer maker has ever offered. Dell's current four-processor server, the PowerEdge 6650, starts at about $9,000.

Dell says the 6800 and 6850, slated for availability in the next few weeks, will provide 32% faster performance than its previous four-way offerings.

The servers come in two configurations: one with an 8M-byte, Level 3 cache, appropriate for data-intensive database applications, and another with a smaller, Level 2 cache, but faster clock speed, ideal for server consolidation and more processor-intensive enterprise applications, says Jeff Clarke, senior vice president of Dell's product group.

The servers are certified to run Oracle Database 10g, Oracle Database 9i Real Application Cluster and Microsoft SQL Server. The servers also will support 64-bit versions of the applications and operating environments as they become available, Clarke says.

The move continues Dell's effort to convince end users to migrate from costly Reduced Instruction Set Computing-based systems to grids or clusters of lower-priced, standards-based servers, he says.

Dell also announced enhanced management tools with OpenManage 4.3, which Clarke says will let users easily update BIOS and firmware.

Dell also is rolling out a Data Center Environment Assessment service to designed to help users address heat and power issues.■

Networx

continued from page 1

Collet, vice president of engineering at AT&T Government Solutions. "We've had some very senior management attention to Networx ... If you look at AT&T's revenue of $36 billion a year, Networx is meaningful."

Networx also is attracting interest on Capitol Hill. The House Committee on Government Reform held its third hearing on the program in March.

Committee Chairman Rep. Tom Davis (R-Va.) said Networx has the "potential to be both the largest telecommunications procurement ever as well as the one that creates the federal government's first digital, government-wide interoperable communications network."

Davis isn't the only one keeping tabs on Networx. The whole telecom industry is watching to see which companies snare this mega-deal.

Run by the General Services Administration (GSA), Networx will replace an expiring series of contracts known as FTS2001. Sprint and MCI hold the main FTS2001 contracts, but Qwest, AT&T, SBC and other rivals hold what are called crossover contracts that let them bid on federal network jobs.

The FTS2001 contracts expire in 2007. To replace FTS2001, the GSA plans to award seven contracts under its Networx program, which is divided into two parts: Universal and Enterprise.

With Networx Universal, service providers will offer domestic and international telecom services ranging from older frame relay and ATM to cutting-edge IP VPNs and VoIP. Universal encompasses 37 services including Web hosting, messaging, managed security, wireless and satellite. GSA expects to award two Universal contracts.

The Networx Enterprise contracts are geared toward smaller, specialized carriers that can't meet the Universal requirements. Carriers must bid a core set of nine IP and wireless services, but other capabilities are optional. GSA says it expects to award five Enterprise contracts.

The GSA released a draft RFP for Networx in October 2004, and it plans to issue the final RFP on April 1. Bids are expected to be due in July, with an award date planned for April 2006.

Dozens of telecom and network companies are angling for a piece of Networx. So far, 40 companies — including service providers, systems integrators and small businesses — have submitted comments to the GSA regarding this program.

Traditional carriers including AT&T, MCI, Sprint, Qwest and SBC are likely bidders on Networx Universal and also are expected to bid on Networx Enterprise.

"It's fairly well understood for companies like AT&T, MCI and Sprint that they have to bid on Universal as the prime contractor," AT&T's Collet says. "If you bid on Universal, the incremental effort to bid on Enterprise is pretty small. God forbid you lose on Universal. Enterprise is your alternative."

Networx Enterprise is expected to attract Verizon and specialized carriers such as Level 3 Communications, WilTel Communications, IDT and Broadwing Communications. Systems integrators including Electronic Data Systems and Computer Sciences also are interested in Enterprise.

"The systems integrators are starting to play a much stronger role in the federal telecom market," says Ray Bjorklund, senior vice president at Federal Sources, a government market research firm. "The systems integrators are picking up capabilities in long-haul and IP-type solutions and integrating them with functional solutions such as supply-chain management and financial management."

The reason so many service providers and systems integrators are interested in Networx is because its predecessor contracts have been so lucrative to the winners. Incumbents MCI and Sprint have racked up revenues of about $3 billion each on FTS2001, industry insiders say.

Sprint, for example, has served federal agencies for 16 years under FTS2001 and its predecessor FTS2000.

"We have over $800 million a year in revenue in the government space, and it grows at a very nice rate for us," says Tony D'Agata, vice president and general manager for Sprint's Government Systems Division. "In 2004, we grew at 24%, which is nice growth compared to the rest of the market."

Networx represents a huge amount of revenue and long-term commitment from a stable customer, which is unusual given the turnover on commercial deals.

Networx has "full attention at MCI corporate from all departments — product development, marketing and engineering," says Susan Zeleniak, vice president of civilian networks for MCI's Government Markets Division. "The opportunity is so significant and includes so many services. It's a model for the kind of integration business that we want to do in the future."

But the way Networx is set up, only a small portion of that estimated $20 billion is guaranteed. The federal government has committed to spend only $525 million on the Universal contracts and $50 million on the Enterprise contracts.

"Networx is a hunting license," Qwest's Payne says. "It's the opportunity to open up many other doors in the federal market."

Bidding on and winning Networx won't come easily or inexpensively. All the telecom carriers say they are investing significant amounts of money to prepare their Networx proposals.

"We've been working on [Networx] for nearly two years," AT&T's Collet says. He says AT&T is making major investments this year in "bid and proposal costs, back-office system development and operational systems development that you have to do in 2005 to get ready for 2006."

Prospective bidders say they will have to make extensive changes to their billing and back-office systems to customize them to meet government requirements. They are urging the GSA to let carriers use the same billing and back-office systems used in their commercial operations.

Verizon estimates that it will cost almost $50 million to upgrade its service order, billing and reporting systems to meet the requirements of Networx Enterprise. This investment will occur even though Verizon already has dedicated billing and provisioning systems for other GSA and federal contracts.

The billing requirements are "a make or break issue for us," says Shelley Murphy, vice president of federal sales for Verizon's Enterprise Solutions Group. "Networx is requiring a different billing system than we have on FTS2001. We are compliant with that as a crossover contract holder. What is occurring is that there are many more billing requirements under Networx and a broader range of services."

Carriers that win Networx will be under pressure to keep their pricing down over the life of the 10-year contract. By awarding seven Networx contracts, GSA's goal is to foster ongoing head-to-head price competition for individual agency requirements.

GSA Administrator Stephen Parry told the congressional committee that "prices on the Networx program must continue to be better than prices available elsewhere in the telecommunications marketplace."

"Networx is largely a set of network components, so prices are going to be very aggressive," Sprint's D'Agata says. "It might be difficult for an integrator or a third-party to be competitive under the current structure."

One major question mark with the Networx program is how it will be affected by ongoing industry consolidation.

AT&T's Collet says his company's pending merger with SBC is not changing his plans regarding Networx. "These mergers will not affect the bids," Collet says. "Until the deals are signed, we are all operating as if we are independent companies."

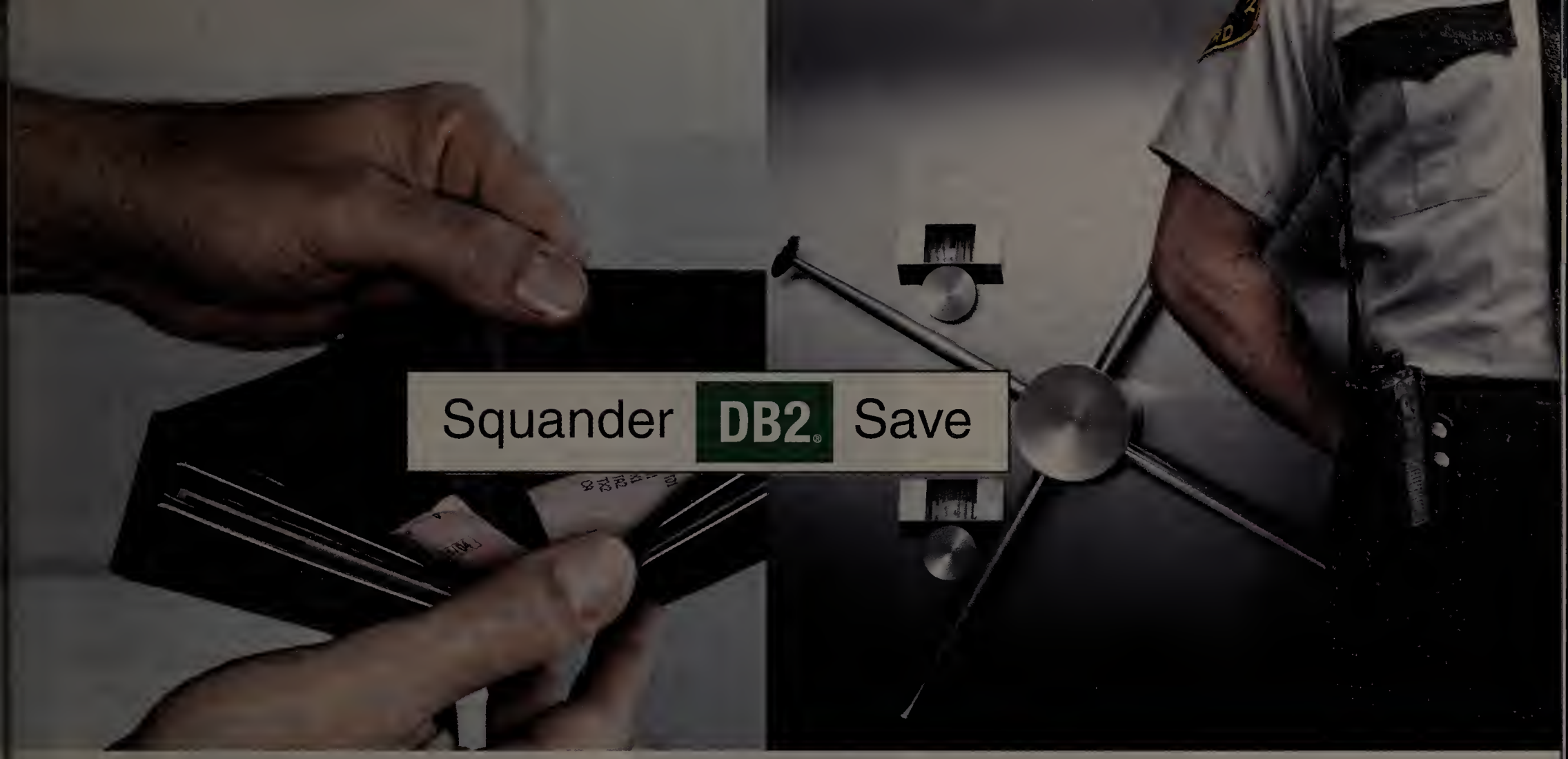
The same is true for MCI, which is being bid on by Verizon and Qwest. MCI earns more than $1 billion per year on FTS2001 and other federal contracts.

"We're just heads down and moving forward on Networx," agrees Jerry Edgerton, senior vice president of government markets for MCI. "We're trying to keep out as much noise as possible during the process."■

Networx at a glance

What is it:	Upcoming federal procurement for telecom services.
Length:	10 years
Estimated value:	$20 billion
Parts:	An all-encompassing Universal program and a targeted Enterprise program for niche services.
Universal bidders:*	AT&T, MCI, Sprint, Verizon, Qwest, SBC
Enterprise bidders:*	AT&T, Qwest, SBC, Verizon, Level 3, WilTel, IDT, Broadwing Communications, EDS, MCI, Sprint and CSC.

* As anticipated by the industry.



DB2. ONLY THE PERFORMANCE IS HIGH.

DB2 has done it again. According to a Market Magic Study, DB2 costs "on average 22% less than Oracle."[1]

The Transaction Processing Performance Council results show that DB2 and eServer™ p5-595 are more than twice as scalable as Oracle Real Application Clusters, making them the overwhelming performance and scalability leader for TPC-C.[2] And an ITG study showed overall costs for Oracle Database up to four times higher than DB2.[3]

No wonder DB2 is regarded as the leading database built on and optimized for Linux®, UNIX® and Windows®. Like other IBM database engine products such as Informix® and Cloudscape,™ DB2 is part of an innovative family of information management products that integrates and can actually add insight to your data.

It takes full advantage of your existing heterogeneous and open environments, while its leading-edge autonomic computing technology means increased reliability, increased programmer productivity and decreased deployment and management costs.

One more thing: Oracle desupported Oracle Database 8i last year, meaning potential headaches, higher cost or a complete migration to current versions of Oracle. Fortunately, IBM offers ongoing, around-the-clock service and support for DB2.

Why not move up to middleware that makes sense? Now you can get IBM DB2 Universal Database or Informix by taking advantage of our extremely compelling trade-up program. Visit **ibm.com**/db2/swap today to find out if you qualify.

IBM

ON DEMAND BUSINESS™

 [1]"Database Comparative Cost of Ownership," January 2003, Market Magic Ltd. [2]All referenced results are current as of 12/14/04. DB2 UDB v8.2 on IBM eServer p5 595 (64-way POWER5 1.9 GHz) and AIX 5.3L: 3,210,540 tpmC @ $5.19/tpmC available: May 15, 2005, vs. Oracle RAC 10g on HP Integrity rx5670 Cluster 64P (16 x 4-way Intel Itanium2 6M 1.5GHz): 1,184,893 tpmC @ $5.52/tpmC available: April 30, 2004; TPC Benchmark, TPC-C, tpmC are trademarks of the Transaction Processing Performance Council. For further TPC-related information, please see http://www.tpc.org/. [3]"IBM Solutions for PeopleSoft Deployment in Mid-sized Businesses Quantifying the New Cost/Benefit Equation." July 2003, International Technology Group, Los Altos, California.

Identity theft
continued from page 1

available at our disposal," says Greg Garcia, vice president of information security at Washington, D.C., trade group Information Technology Association of America, which backs the idea of a national law applicable to all "data custodians."

In response the Federal Reserve, in cooperation with other regulatory agencies, last week issued rules that require banks to adopt a risk-based response program to address incidents of unauthorized access to the customer information they electronically hold.

The new rules are contained in an advisory titled "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." Jointly issued by the federal government's primary regulatory agencies for banks — which include the Federal Reserve and the Federal Deposit Insurance Corp. — the requirements meet data-privacy and protection guidelines called for in the Gramm-Leach-Bliley Act passed by Congress in 1999.

The rules make clear that banks — though not stock brokers, credit unions, insurance companies or investment firms — must notify customers "as soon as possible" by e-mail or written letter of "an incident of unauthorized access to sensitive customer information," defined as Social Security numbers, accounts and the other detail, according to sources at the Federal Reserve.

Under the new regulation, banks can only delay this notification by working with a law-enforcement agency that determines whether notification would hinder a criminal investigation.

Like the California Online Privacy Protection Act of 2003, which requires disclosure when a California resident's personal data is compromised, the federal guidelines for banking are likely to force more public disclosures.

A high-tech fix?

Businesses are worried they could be next, and some are deploying new technical security protections.

At Irving, Texas, medical staffing and recruitment firm Martin, Fletcher, Vice President of IS Fabi Gower says the firm maintains a 15G-byte database of private information full of personal information about doctors, nurses and other professionals.

The staffing firm has an established written policy for its employees on how data should be kept confidential, but Gower said she wants to enforce it through technology. "I was feeling desperate for a solution to this," she adds.

To that end, the firm installed SecureWave's Sanctuary Device Control software on employee laptops and PCs to prevent the use of a wide range of devices that might be used to steal data. That would include CD/ROMs, wireless LAN adapters, digital cameras, printers, scanners and USB memory sticks. "We can control every single PC or tablet centrally," Gower says. The company also monitors content via WatchGuard's Webwasher product.

Next week, Centennial Software is expected to come out with a competing desktop software product, called DeviceWall, that can be centrally managed. The software can be configured to lock down the use of removable media devices, PDAs, smart phones, optical drives and music players.

The software, which costs $20 per seat and ships in early April, is intended to thwart data theft by closing down easy access to the wide range of storage devices that have come on the market, especially in the last six months, the company says.

Tizor this week will debut with a content-usage monitoring appliance called the TZX 1000. The start-up, founded by former Bell Labs researchers, says its appliance can sit in front of any database, file system or application server and detect identity theft.

These are high-tech and low-tech ways in which thieves steal identities, according to the Federal Trade Commission.

- Getting information from your employer by stealing records; bribing or conning other employees; or hacking into computers.
- Rummaging through trash.
- Obtaining credit reports posing as a legitimate requester.
- Stealing credit and debit cards from wallets or by using an information storage device in a practice called "skimming."
- Completing a "change of address form" to divert mail.

"It's using data mining as applied to security," says Prat Moghe, founder and CEO. "It picks up telltale signs, such as high-volume disclosure or noticing that someone is looking at content they never looked at before."

Tizor has no customers it will disclose for the TZX 1000, which starts at $50,000.

Pete Lindstrom, an analyst at Spire Security, says detecting when an authorized user — or someone who has stolen an authorized user's password — is accessing data for fradulent purposes is difficult. Tizor's appliance might simply act as a deterrent, he says.

But Moghe says that Tizor is not prepared to guarantee that its product would detect all occurrences of online data theft.

Ambeo, Guardium, Lumigent, IPLocks and Application Security are other vendors with products that watch databases and servers for content misuse.

A few, such as Verdasys, have desktop software that monitors what users pull from databases. Another category of content monitor focuses on having a gateway watch for sensitive data, such as Social Security numbers, and whether they are being sent over the Internet. Vontu, Tablus, Vericept, Reconnex and Vidius all have gateway-style products, which keep watch for unauthorized content transmissions.

According to Gartner analyst Rich Mogull, content data-monitoring products aimed at foiling data theft are not yet in widespread use. While various products certainly can't hurt in stopping identity theft, he says the problem is unlikely to be solved through technology alone.

"Our credit system is set up to fail," Mogull says, adding that the current method widely used for making financial credit available to consumers relies far too much on Social Security numbers and date of birth as the key means to verify a person's identity. He says there needs to be a long look at finding alternate methods of identification. "We need to change the system," he says. ■

Mgmt. features key to SSL VPN pack

■ BY TIM GREENE

Permeo Technologies this week is introducing software that it says makes managing SSL-based VPNs simpler.

The NEC spinoff has developed software to scan computers for security compliance and for cleaning out data accessed during remote sessions, and has integrated management of these features. Vendors that partner to provide similar features require customers to employ multiple management consoles, Permeo says.

Called Base 5, the company's software scans computers as they try to access corporate VPNs to check that they have properly patched operating systems, updated anti-virus software and that a personal firewall is running. It continues to check the computer throughout the remote session to make sure it remains compliant, just in case the user tries to turn off the firewall, for instance.

Data displayed during a VPN session is purged and cannot be transferred to files on the computer. This prevents confidential data from remaining on the machine for later users to see.

The software also can protect against the action of malware by whitelisting applications the remote computer can run during a session. This feature effectively blocks malicious executables such as Trojans and worms, the company says. The software can also blacklist specific, non-malicious applications such as Kazaa that network executives don't want used during VPN sessions.

These features parallel those offered by SSL VPN vendors such as Check Point, as well as Aventail and Juniper, which both partner with Sygate for endpoint security.

Lee Lewis, IT operations manager at Summit Electric, says Base 5 is easier to use than Permeo SSL Remote Access, which the Albuquerque, N.M., company has used for two years.

"It doesn't require a separate application menu that is confusing," he says. Instead, end users are presented with client applications that look as they would on their LAN desktops.

Base 5, which includes a hardened Linux operating system, costs $50 per user for more than 1,000 users, $75 per user for 250 to 1,000, and $100 per user for less than 250. ■

Q&A

Your take

Network executives share their wisdom

Paper maker documents key IT security issues

James Cupps, a former network engineer and information security officer for the U.S. Navy, is now on his second tour of duty with Sappi Fine Paper North America, a division of a $4.7 billion South African manufacturing company. Cupps, the North American division's information security officer and Sappi's global security lead, recently shared his thoughts with Network World *Executive News Editor Bob Brown.*

Give us a feel for your job responsibilities and the company's network.

Overall, we have 20,000 employees but only about 10,000 systems that are spread over several hundred subnets. In North America, we have about 300 systems and about 4,000 employees. We have offices on six continents, with large-scale manufacturing presence on four. I am responsible for network and application security including segregation of duty in our ERP system, anti-virus, edge protection, disaster recovery, policy creation and enforcement, regulatory compliance/[Sarbanes-Oxley] and business continuity.

What's the most underappreciated aspect of your job?

Building interregional and interdepartmental consensus.

How is overseeing IT security at a corporation different than in the military?

Believe it or not, you can make decisions more quickly and get them enacted faster in a company. There is more focus on disaster recovery/business continuity in a business and more focus on edge security and general data classification/protection in the military. Other than that, there are a lot of overlaps.

On one hand more threats, from viruses to phishing to spyware, are hitting networks. On the other hand, more money is being sunk into security companies and more tools are coming out. Is it getting any easier to sleep at night?

Actually, yes. The bad guys are definitely getting better, but so are the vendors. Some of the newer [intrusion-prevention system (IPS)] mechanisms are quite easy to deploy and manage and are remarkably resilient. If you implement them in a smart-layered architecture the cost isn't much higher than what we have seen over the last several years. Add to that the fact that executive management is giving the area substantially more attention, and it is finally possible to get real problems fixed. There are a lot of tools, strategies and mechanisms for dealing with rights issues such as [separation of duties] now that had to be performed manually — or more likely not at all — just a few years ago. There are still a few things that worry me. Process-control security is getting a lot more attention but still needs more work from manufacturing companies and the makers of the equipment. This is the infrastructure that allows actual physical control of machinery and plant equipment.

Network security consultants and vendors are fond of painting a frightening picture of network security threats — viruses that result in planes crashing or patients getting the wrong medicine. How real are such threats to you?

I don't know about planes or hospitals. In factory settings, there are fail-safe settings that help avoid safety issues. It is possible to interrupt manufacturing, though, and poor facility design might allow for worse events. People need to realize two things: First, it is always possible for good operators to manually step in and interrupt a problem, so the worst case scenarios are not as bad as what you see on prime time TV. Second, more equipment is being connected directly to IP networks so even if manual operations can stop problems, it is still getting much easier for hackers, viruses and worms to cause problems for modern facilities whether they are power companies, oil producers or paper manufacturers.

There's a lot of talk these days about the borderless perimeter — the idea that it's getting more difficult to define your network's perimeter. What are you seeing here?

Whether we like it or not, the increasing ease of communications and the need to provide access to outside vendors, contractors and partners is slowly eroding what has traditionally been the primary line of defense. This doesn't mean you don't need edge protection; it means you need to redefine what an edge is. You still need the firewall and/or a network IPS, DMZ and extranets, but now the DMZ and extranets might be distributed over multiple points. You need to have layered defense.

What's the smartest thing your company has done to ensure network security?

The deployment of host-based IPS and a comprehensive intrusion prevention/anti-virus monitoring and control environment. We have caught and cleaned many viruses that we couldn't even see with our old system, and we have been able to better coordinate our patch process instead of just reacting.

What role, if any, should government play in helping companies out with their IT security?

As little as possible and only informational. They just aren't the real experts. Well, most of them.

What impact has Sarbanes-Oxley had on your IT department?

It's had a very large impact, and we have devoted a significant amount of resources to ensuring we are compliant both in spirit and in the letter of the law. We are cooperating with our outside accountants and meticulously identifying our controls and system security settings.

How much attention are you paying to identity management?

To have an adequate control infrastructure you need good identity management. Our primary early focus is on segregation of duty within financial systems, but we also have adopted solutions and policies for other aspects of ID controls and management.

It can be hard to get companies to talk publicly about their IT security strategies and challenges for obvious reasons. But what can corporations do to warn each other of new threats and generally help each other out?

It is important to participate in external forums and discussions. There are pieces of information that are best kept private, but security by obscurity doesn't work.

What's your take on Microsoft's security efforts these days?

They are making an honest effort, but they still often miss the big picture. The fact is they are in a no-win situation. Their phenomenal success has made them effectively the only target worth pursuing. I don't think it is fair to compare them to other [operating systems] in

See Cupps, page 64

Getting

Title: Information security officer

Organization: Sappi Fine Paper North America

IT staff size: About 20, including a four-person security staff, manager of operations and service desk manager.

IT budget: $7 million

Job history: Six years at Sappi; worked as a penetration tester for consulting firm MarchFirst; was network engineer and information security officer for Commander Northeast region of the U.S. Navy.

If he wasn't in IT security: "I'd probably be a salesman; I have a knack for a pitch."

Fun fact: Is a qualified nuclear reactor operator; has five children.

Last good book read: *Cryptonomicon* by Neal Stephenson.

More online! www.nwfusion.com
For more of the interview, head online. **DocFinder: 6447**

DAVID WADE

WE KEEP YOUR PEOPLE MOVING WITHOUT SHAKING THINGS UP AT THE OFFICE.

Soon, over 99 million employees worldwide will be working outside the office.[1] Is your communications infrastructure ready? It will be with Avaya IP Telephony. Give your employees the capability to work from the road, at home, anywhere—with advanced solutions that are easy to use and simple to maintain.

Keep your existing network up and running. Avaya lets you leverage your existing technology in a multi-vendor environment, so you can migrate your IP deployment with confidence.

Secure? Absolutely. Our industry-leading, end-to-end media encryption protects each IP call. Avaya experts help you design, seamlessly implement, manage, and maintain your network for fully optimized performance. As the award-winning leader in IP telephony,[2] and with our unique approach of embedding communications at the heart of your business, Avaya is the perfect partner to help keep your people connected, no matter where they are.

GET STARTED AT WWW.AVAYA.COM/MEANSBUSINESS—WITH A FREE WHITE PAPER "BEST PRACTICES FOR IP DEPLOYMENT IN A MULTI-VENDOR ENVIRONMENT."

Or call 1-866-697-5566 to speak to a representative.

AVAYA

COMMUNICATIONS
AT THE HEART OF BUSINESS

- IP Telephony
- Contact Center
- Mobility
- Services

[1] Gartner Dataquest, *Teleworkers: The Quiet Revolution*, September 2004. [2] Wainhouse Research, "Business-to-Business Test in Large Enterprise IP PBX" 2003.

Net Infrastructure

■ SECURITY ■ SWITCHING ■ ROUTING
■ VPNS ■ BANDWIDTH MANAGEMENT
■ VOIP ■ WIRELESS LANS

Force10 switch targets data center

■ BY PHIL HOCHMUTH

Force10 Networks this week will release its first fixed-configuration switch aimed at data center customers looking for a high-capacity box for linking a server rack to a 10G backbone.

The company says its S50 switch has capacity and resiliency features beyond stackable switches from other vendors, which are meant for wiring closets but are often used for hooking up server racks in data centers.

Port-wise, the S50 stacks up against competitive fixed-configuration devices — it includes 48 10/100/1000M bit/sec ports, and uplinks include slots for four 1 Gigabit and two 10G modular fiber ports. Observers say the 190G bit/sec switch fabric inside the S50 is what separates its data center stackable switch from other wiring-closet-focused stackable switches.

"This product is meant to connect racks of servers with dual [Gigabit Ethernet network interface cards] to a 10G backbone," says Andrew Feldman, Force10's vice president of marketing. "It's not for connecting desktops and printers."

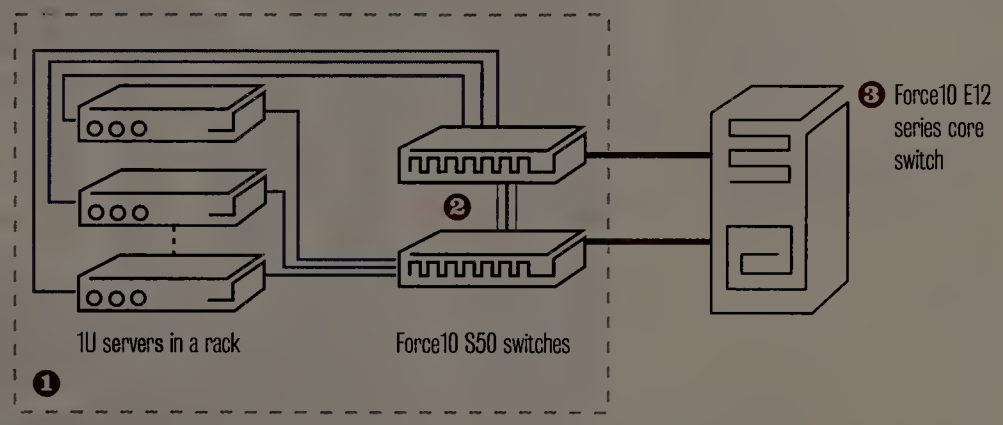
The switch supports full Layer 3 routing, which lets users connect rack-mounted servers to two different S50s in a rack. With this "dual-homing" technique servers are given redundancy and increased throughput, Feldman says. The switch also supports a proprietary stacking technology, which lets two to eight S50s link in a stack with a virtual 20G bit/sec backplane. The stacking technology also lets multiple S50s be managed with one IP address.

Force10 also has pushed down to the S50 the same Layer 2/3 switch resiliency technology in its core chassis lines. This architecture separates the functions of Layer 2 and Layer 3 into separate ASICs and provides redundant silicon in the switches. Redundant silicon lets the box continue forwarding packets in case of component failure or if a processor becomes overtaxed — such as broadcast storms or bandwidth-flooding network

See Force10, page 18

Racked up

Force10's S50 switch is designed to link many servers to a 10G data core center.



1. Servers with dual Gigabit NICs connect to S50 switches.
2. Full Layer 3 routing lets users link 48-port S50 switches to multiple servers in the rack, offering redundant, routed paths. A proprietary stacking cable lets S50s share a 20G bit/sec backplane.
3. Dual 10G uplinks and four ports of Gigabit fiber hook the server switches to modular 10G core boxes.

Short Takes

■ Web security vendor **Layer 7 Technologies** and **Tarari,** which develops XML acceleration processors, said last week that they will work together to develop **XML Firewall Blade** for IBM eServer BladeCenter. The blade will focus on security and processing XML traffic. It combines Tarari's XML silicon with Layer 7's policy processing and enforcement operating system. The Layer 7/Tarari blade is one of three XML security and acceleration products the duo plan to introduce this year. The Firewall Blade is expected to be available in May.

■ **NEC** last week said it is developing a **network security system** that will monitor and analyze the configuration of security tools deployed in a network and suggest changes to fix vulnerabilities and any redundancies between them. The system is intended for use in networks where a mix of security tools, such as firewalls and intrusion-detection systems, are being used to guard against worms, viruses and other malicious traffic. As servers and client computers are added and removed from networks, and as security tools are installed or taken away, security holes, redundancies and other "mismatches" can appear in the tools being used. NEC's product, which still is being developed and might not go on sale until early next year, collects and analyzes the configuration parameters of the security tools in a network to detect any holes or overlap between them. The system uses a language called Security Configuration Coordination Markup Language, which describes the filtering and monitoring functions of firewalls and IDSs, NEC said.

Start-up offers high-capacity WLAN gear

■ BY JOHN COX

A start-up this week is unveiling a super wireless LAN access point that can offer greater capacity and more coverage than conventional access points.

The Xirrus XS-3900 Wireless LAN Array combines advanced antennas, up to 16 802.11a radios and a WLAN switch in a package that looks like an oversized smoke detector. Xirrus software coordinates the 16 WLAN radios to boost capacity. That's because users can connect to the array on 16 channels at the same time, each channel with a data rate of 54M bit/sec, compared with just one channel on a conventional, one-radio access point.

The effect is somewhat comparable to taping together 16 802.11a access points, but adding a special multi-sector antenna that directs the radio energy thereby extending its range, and adding some clever software that blocks interference between the radios and lets users use adjacent channels, again without interference.

Xirrus' XS-3900 Wireless LAN array can support up to 864M bit/sec of bandwidth.

One of the 3900 arrays is being used to cover a two-story, 7,800 square foot classroom building on the campus of the Viewpoint School, an independent K-12 school in Calabasas, Calif. The single array mounted centrally on the second floor ceiling handles coverage for the entire building and extends the WLAN roughly 150 feet outside the building, which covers part of the campus, says Paul Rosenbaum, the school's associate headmaster, COO and director of technology.

Previously the building had four Cisco Aironet access points to cover the same area with adequate performance.

Rosenbaum already is weighing the use of the array in a new 40,000 square foot building under construction because the Xirrus products will reduce WLAN installation and maintenance costs. "Lots of client

See Xirrus, page 18

TOLLY ON TECHNOLOGY

Kevin Tolly

Identity theft, data security, back-up services

In mid-March, lawmakers in Washington were busy grilling executives from Bank of America, ChoicePoint and LexisNexis about recent breaches of security that led to personal data of hundreds of thousands of people ending up in the wrong hands. In most cases, the data had gone out "through the front door" as it were — with criminals masquerading as legitimate users of ChoicePoint and LexisNexis services. As they all now race to guard the front door, I couldn't help but think about the new "back door" (being built into many businesses) — third-party back-up services.

As the current examples (and many others) illustrate, it is difficult enough to protect data when one has complete control over it. With the surge in popularity of third-party online back-up services, how will that complicate an already-complex issue?

For decades, "backup" meant spooling off tapes, managing various media and retention dates and, ultimately, shipping back-up tapes to physically secure locations using the services of a company such as Iron Mountain.

Recently, though, companies such as LiveVault came on the scene to offer services that eliminated the tape and the travel by backing up your disk to their disk over a WAN connection. In one stroke, they solved the "offsite" problem (i.e., needing an emergency copy at a safe location) and the myriad issues related to tape management. Tape, of course, remains a vitally important component of backup, but that's another column.

But — and you knew that was coming — putting a third-party back-up company into the mix creates at least the possibility of a back door through which data can be compromised.

Interestingly, there is a LiveVault LexisNexis nexus. Last September, LiveVault announced that LexisNexis would offer the former's services to the latter's legal and business customers.

So let's play what-if and run through some hypothetical scenarios using these companies as placeholders:

While data transmitted to a LiveVault can be encrypted across a VPN, it would appear that when the data reaches the "secure, remote facility," it sits on the disk in all its unencrypted glory. I don't know of many small businesses or law offices that keep their data encrypted on their in-house servers.

I could be wrong, but I couldn't find any reference on LiveVault's site that declared that the stored data was safe from any potential miscreants who happened to have access to the "secure location."

In theory at least, someone either hacking into said location or a criminally minded data-center employee could walk off with a goldmine of data. After all, providers of online backup are likely handling data for perhaps hundreds of companies.

So should something get out through the back door, which of the companies involved is liable for the damage incurred?

If you are the law firm whose records have been compromised, do you sue LexisNexis or LiveVault? This being America, of course you'd sue both and anyone else that you could think of.

And one wonders what their response would be. Would they simply try to put the blame on you saying that you should have stored sensitive information encrypted? Probably.

Given the growing popularity of these services, it would be nice to see prospective customers asking these tough questions and vendors addressing these issues head on.

Tolly is president of The Tolly Group, a strategic consulting and independent testing company in Boca Raton, Fla. He can be reached at ktolly@tolly.com.

Xirrus

continued from page 17

devices can associate with one [Xirrus] device. That's a huge plus," he says. Using the Xirrus DC power option will eliminate the need to install AC power lines to each array, he says.

"We'll be reducing cabling, the number of switch ports needed in the wiring closets and power cords," he says.

The array comes in four-, eight- and 16-radio models. Picture an 18-inch dinner plate with the radios mounted around the diameter. The array can have up to 12 802.11a radios and up to four dual-frequency radios, which can support either 802.11a or 11b/g clients.

Each radio has a sectorized antenna, which in effect, concentrates the radio's energy in a specific segment, or sector, instead of letting it radiate in all directions as in a conventional access point. By concentrating the energy, the array extends the radio's range, so that at any given distance, the available WLAN throughput is higher than a conventional device. Xirrus executives say that the typical range for an 802.11a access point is less than 100 feet, but the array can reach 175 to 200 feet. The company says the array has about twice the range, at any given data rate, of rival access points from Cisco, Aruba Wireless Networks and Trapeze Networks.

One radio can be designated as a radio monitor, constantly sweeping the airwaves to check signal strength and detect unauthorized WLAN signals.

The built-in WLAN switch, which Xirrus dubs the array controller, is where the magic occurs. The switch carries Xirrus software that creates a media access control layer that spans all the radios, instead of each radio having its own MAC address as in conventional access points. In effect, the Xirrus software creates one radio with 16 channels, all of which can operate at the same time.

The switch has two Gigabit Ethernet uplinks to connect upstream to the nearest wiring closet switch. To handle the traffic load, encryption processing and other tasks, it's powered by a 800-MHz PowerPC CPU, with 640M bytes of double data rate RAM.

A separate box, in various models, slots into a data center rack mount to manage 10 to 500 arrays via a GUI. This management system handles configuration, authentication, security policies and firmware upgrades. Xirrus supports the usual security standards: 802.1x for authentication, and 802.11i for security and encryption. The array works with back-end RADIUS servers.

Finally, the array supports 802.11e for QoS capabilities, and standard alphabet soup of security.

There is a DC power option: another rack-mounted box can power the array with DC power over a separate Category 5 cable or 16-gauge wire.

All products will ship in May. The list price for the array starts at $4,000 for the four-radio 3500 model. The eight-radio 3700 array costs $7,000; the 16-radio 3900 array costs $12,000. The management models range from $5,000 to $25,000, depending on the number of arrays being controlled. The remote power system starts at $2,000 for the chassis and one expansion module, which powers four arrays. ■

Software tackles spyware, virus threats

■ BY ELLEN MESSMER

Start-up GreenBorder Technologies last week debuted software aimed at preventing spyware and virus contamination from the Internet for users of Microsoft's Internet Explorer browser and Outlook e-mail.

The company's first product is GreenBorder Professional Edition, desktop security for Internet Explorer and Outlook that ships with a centralized management console and forensics tools to distribute and configure the software.

GreenBorder — so called because its products wrap a green border around the user's screen whenever the user is on the Internet rather than an internal network — says its software wards off Internet-originating malware and unwanted file downloads through a barrier process.

GreenBorder doesn't view its software as a substitute for antivirus or intrusion-prevention systems, and at least one beta user agrees.

"We have anti-virus, too, but we're using GreenBorder on 250 computers as an additional security," says Anthony Shields, a systems administrator with The Epstein School, a private elementary and middle school in Atlanta. "GreenBorder doesn't hinder Internet access. If you want to download a program file, for instance, it recognizes you're choosing to save it. But it will block things you don't intentionally want to download."

The software runs on Windows XP Professional and Windows 2000 Professional. GreenBorder professional Edition starts at $59.95 per seat, plus about $5,000 for the centralized configuration and reporting software. ■

■ More GreenBorder news can be found in the Network Life supplement. PAGE S-6

Force10

continued from page 17

attacks. This architecture lets network attacks or failures that would specifically affect Layer 2 not interfere with other Layer 3 traffic, and vice versa, Force10 says.

The S50 will be a good fit in large companies that use Force10 backbone switches and are looking to extend the company's technology to server connectivity, on observer says.

"Force10 is not going after just generic enterprises," says Zeus Kerravala, an analyst with The Yankee Group. "Their stuff is targeted at very dense environments with lots of servers" and Gigabit Ethernet and 10 Gigabit ports. Having the same switches in the data center core and in server racks could make management and configuration easier for data center administrators, he adds.

Force10 users will probably find that having a common operating system and configuration tools in switches in server racks and the data center core is useful, Kerravala adds.

The device targets such competitive boxes as Extreme's Summit 400 series, Foundry Networks' Fast Iron and Edgelron switches and HP's ProCurve 3400 box.

The S50 will be available in April starting at $8,000. The two-port 10G Ethernet uplink module also will be available in April for $6,500. To upgrade the switch to full Layer 3 switching capabilities, an extra $2,000 software image is required. ■

THE EXPERT'S GUIDE TO THE CONNECTED HOME

NetworkLife™

KEEP OUT

AN EXPERT'S GUIDE TO HOME NET SECURITY

Does your **spyware cleaner** miss the mark?

Plus:

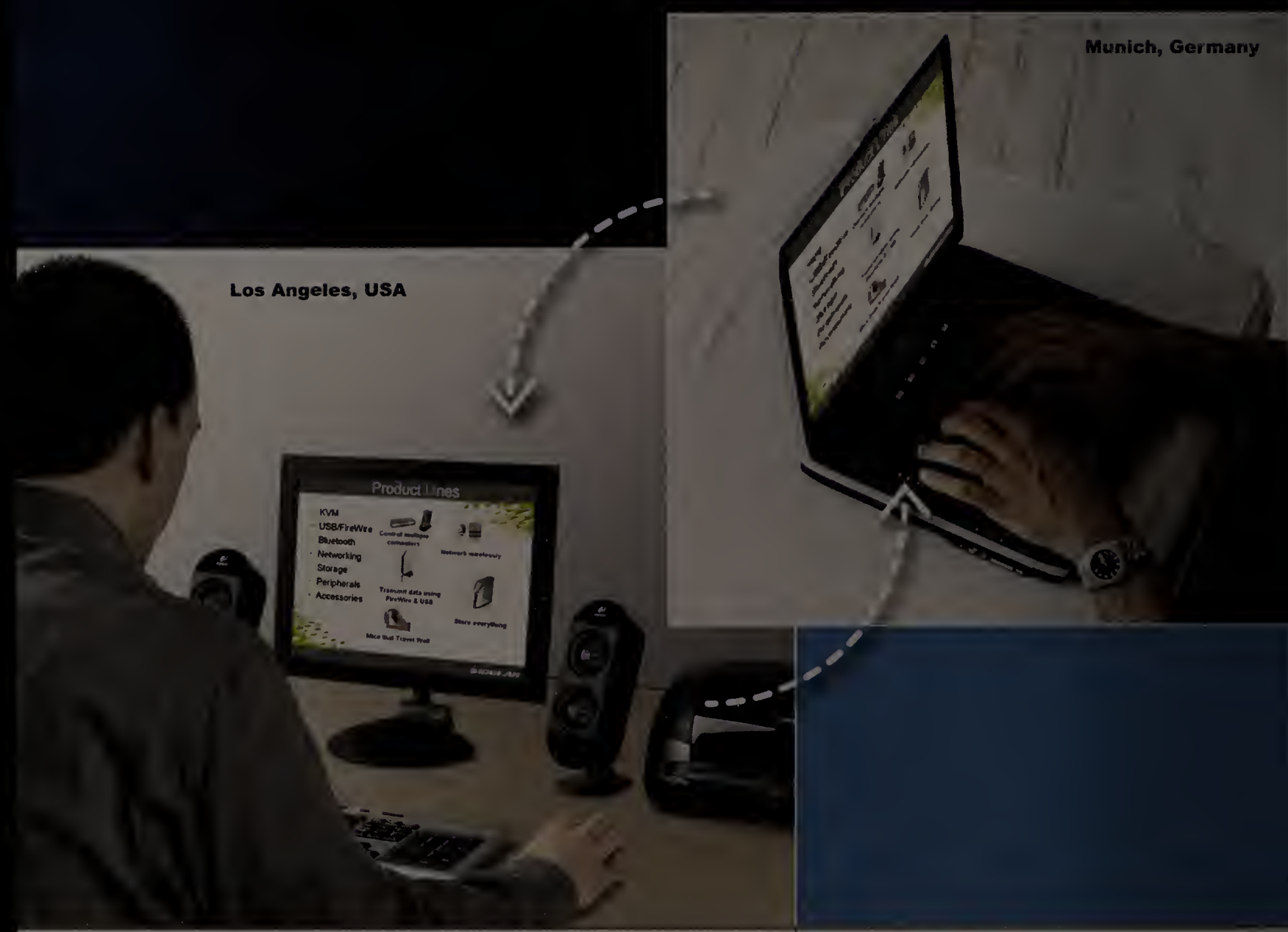
- First SOHO managed security router
- PlumChoice answers PC distress calls
- Phishers catch a break from ICANN
- GreenBorder guards against bad behavior

SimpleShare NAS reviewed

LucidLink Wi-Fi Security

Netgear plugs wireless holes

Share information around the world from your home or office computer - real time



Need to deliver a presentation to a client half-way around the world - real-time? Or collaborate on a graphics file, co-write a script, or devise a marketing plan with a colleague?

ATEN's KVM on the Net™ gives individuals and groups the opportunity to work together in real time, no matter how far they are from each other.

KVM on the Net™ is an IP-implemented KVM solution that delivers access to computers from any system connected to the Internet.

Utilizing advanced security technologies, KVM on the Net™ provides password protection, advanced encryption technologies, sophisticated user filters and management, stealth mode and automatic lockout to make sure that remote access is secure.

Remove time, distance and personnel barriers, while creating new business opportunities worldwide from your home or office. Get KVM on the Net™ today!

CN6000 - KVM on the Net™

Take a Test Drive Over IP Today
Email us at: info@aten-usa.com
or call 1-888-999-2836

ATEN Technology, Inc. | 23 Hubble Irvine, CA 92618 | 1-888-999-ATEN (2836)
Visit us at www.aten-usa.com

ATEN
Simply Better Connections™

Inside:

Editor: **Toni Kistner**
Technology Editor: **Keith Shaw**
Art Director: **Brian Gaidry**
Designers: **Steve Sauer, Tom Norton**
Online Designer: **Zach Sullivan**
Copy Editor: **Monica Hamilton**

From the editor

When it comes to home network security, it looks like things will get worse before they get better. But better — if not downright good — is just around the corner.

Most of the SOS calls you're getting from friends and family are for spyware. PlumChoice, an online tech support company, credits spyware for 40% of its business. Phish attacks are on the rise, and now that ICANN's approved the use of international top-level domains, phishers are having an easy time making fake URLs look real.

I added a Zyxel Homesafe Parental Control wireless router to my parents' broadband PC at Christmas. On a recent visit, my dad says, "You know, that thing you did isn't working anymore. The pop-ups are back."

True, this isn't a fight won by a single blow.

That's why we've devoted much of this issue to the strategies, tactics and weapons you need to win the war — for yourself, users and the community. If the Internet suffers a devastating attack as predicted, we know it'll probably be your dad or mine who unwittingly helps bring it about.

The good news? AOL provides security software to members for free. And new products might make all this just a bad memory. Electronic Lifestyle Integration's $199 security appliance includes a $10-per-month managed service that handles the updates and monitoring for you. And GreenBorder's new software isolates users' Internet activity from the desktop, flushing all code, files and cookies on shutdown.

Speaking last fall at a Bentley College event, former White House Cybersecurity Advisor Howard Schmidt said, "We've learned how to make PCs easy to use but not safe. But it's like driving and seat belts. First, people wouldn't wear seat belts. Now they wear them, and we have laws to ensure they wear them."

So for now, we need to remind our home users to wear their seat belts, or strap them in ourselves.

— Toni Kistner
Editor
tkistner@nww.com

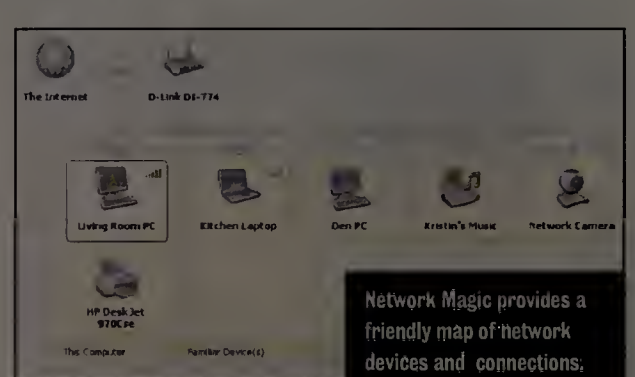
NEWS

- Networks that fix themselves
- Highway Wi-Fi causes near-crackup
- GreenBorder software neutralizes malware

Sticky notes

New tools ease home net headaches

SingleClick and Pure Networks vie to handle configuration and troubleshooting.



Network Magic provides a friendly map of network devices and connections.

At last, home network management tools to the rescue! Two start-ups — Pure Networks and SingleClick Systems — each has just shipped software that eases network configuration and management, and handles basic troubleshooting. Think of them as mini network operating systems that sit on top of Windows. (Neither works with Apple or Linux systems.)

Coming off a beta trial with more than 6,000 users, the Seattle company Pure Networks has released Network Magic 1.0. The software — which you install on each PC — provides a dynamic map of all the devices on the home network. It monitors connectivity and fixes problems behind the scenes. File and printer sharing is automatic, too; simply select resources to share on one PC to make them available to the other PCs.

Corporate laptops are hidden from other PCs on the network, and when the laptop user shares files with other users on the home network, those file shares are locked down when the laptop is removed and plugged back in to the corporate LAN. The product alerts you when an unauthorized person accesses your wireless network, and an upcoming remote-access feature lets users access designated folders from a Web browser.

Network Magic costs $50 for up to five PCs and any number of devices. The product is free to AOL users and integrated into some D-Link Systems routers. Expect Network Magic to make its way into other manufacturers' gear.

After a beta test with about 2,000 users, SingleClick of Toms River, N.J., is releasing HomeNet Manager 2.0 (which costs about $36 for two to nine PCs). HomeNet Manager offers a similar home network map that shows actual rooms, performs the same troubleshooting tasks and simplifies file and print sharing. The product is stand-alone — no bundling deals with hardware vendors or service providers. SingleClick also offers remote file-sharing services for sharing photos, music and other data across the Web. The basic peer-to-peer service, which requires you to keep your systems running and HomeNet Manager active, costs $4.95 per month. The hosted service costs $9.95 per month. ■

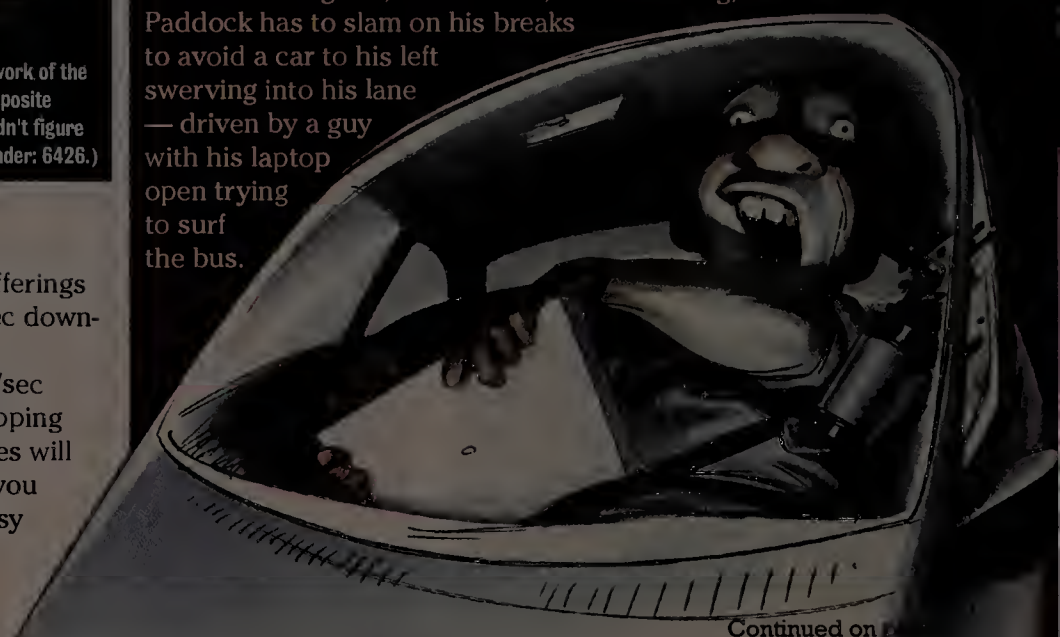
This 1954 photo circulating recently was billed as the home network of the future as envisioned by Rand Corp. Turns out, it's actually a composite image of the helm of a nuclear submarine. Good thing — we couldn't figure out that steering wheel, anyway. (See www.nwfusion.com, DocFinder: 6426.)

Broadband boost

To gear up for a new suite of online service offerings this year, Comcast has upgraded its 3M bit/sec downstream/256K bit/sec upstream service to 4M bit/sec/384K bit/sec. It's upgraded the 4M bit/sec downstream/384K bit/sec upstream to a whopping 6M bit/sec/768K bit/sec. New Comcast services will include video e-mail, an application that lets you create slideshows with digital photos, a fantasy football game and more than 100 games on demand.

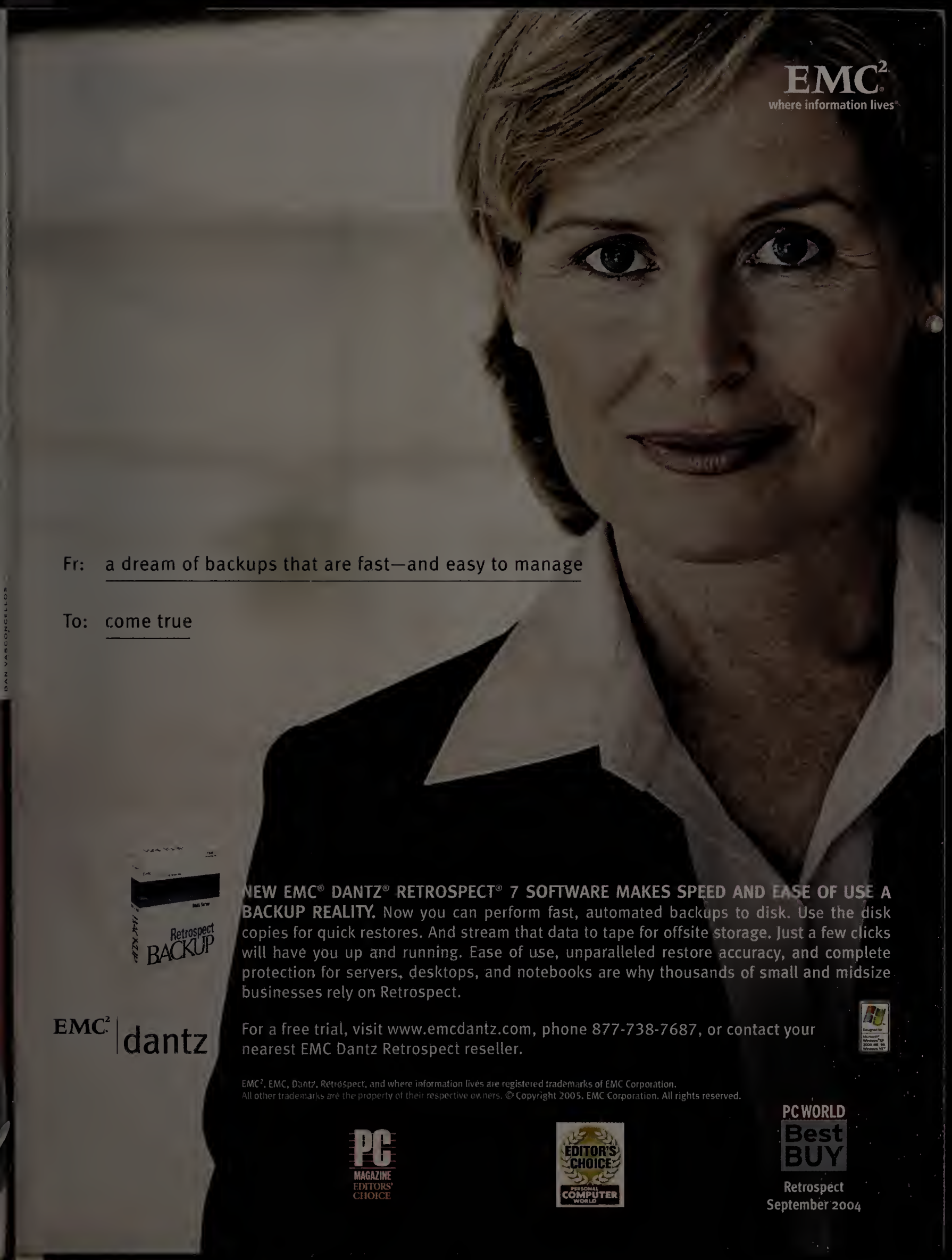
Why they call it war driving

Go-to guy Scott Paddock has seen the future, and it's going to raise your insurance premiums. Driving to his day job as an IT consultant at the Daniels Fund in Denver, Paddock comes upon a commuter bus on Route I-25N with a big sign on the back at eye level advertising "high-back cushion seats, luggage racks and free wireless Internet service." As Paddock tails the bus, temptation sets in, and he considers popping open his laptop to check his e-mail. But before he can get it, one-handed, out of the bag, Paddock has to slam on his breaks to avoid a car to his left swerving into his lane — driven by a guy with his laptop open trying to surf the bus.



DAN VASCONCELLOS

Continued on p


EMC²
where information lives
Fr: a dream of backups that are fast—and easy to manage
To: come true
DAN VASCONCELLOS
Retrospect BACKUP
EMC² | dantz
NEW EMC® DANTZ® RETROSPECT® 7 SOFTWARE MAKES SPEED AND EASE OF USE A BACKUP REALITY. Now you can perform fast, automated backups to disk. Use the disk copies for quick restores. And stream that data to tape for offsite storage. Just a few clicks will have you up and running. Ease of use, unparalleled restore accuracy, and complete protection for servers, desktops, and notebooks are why thousands of small and midsize businesses rely on Retrospect.
For a free trial, visit www.emcdantz.com, phone 877-738-7687, or contact your nearest EMC Dantz Retrospect reseller.
EMC², EMC, Dantz, Retrospect, and where information lives are registered trademarks of EMC Corporation.
All other trademarks are the property of their respective owners. © Copyright 2005. EMC Corporation. All rights reserved.
PC MAGAZINE EDITORS' CHOICE
EDITOR'S CHOICE PERSONAL COMPUTER WORLD
PC WORLD Best BUY
Retrospect
September 2004

PC SOS? Call Plumchoice

Good home network tech support to ease your burden.

When you can't save the day, point your users to PlumChoice for PC emergencies. The Bedford, Mass., start-up provides online technical support and disaster recovery using a combination of phone support and PC remote control (based on Citrix GoTo Assist) to fix PC problems while your users follow along. The service costs $23 for 15 minutes; $80 per hour; and $225 for three hours. PlumChoice also offers onsite support for $119 per hour and drop-off service in its Bedford and Rumford, R.I., locations for $90 per hour.

PlumChoice fixes point problems and makes recommendations. "If a customer calls with a 4-year-old PC, we'll help him buy a new one rather than spend four hours on the phone," says PlumChoice CEO Ted Werth. "If his system is riddled with spyware, we'll recommend Firefox or a spyware application. We'll then download and configure it for him on the spot," Werth says. "We're trying to help people cut down the number of times they call us, even if it means we lose money."

PlumChoice's 30 technical support representatives work remotely all over the country. Most people call PlumChoice with a specific problem. Others have a laundry list of items that need fixing. Werth says security problems account for 60% to 70% of PlumChoice's business, with 40% related to spyware. Only 5% to 10% of calls are to help with a home network, and 15% to help with a virus.

www.plumchoice.com

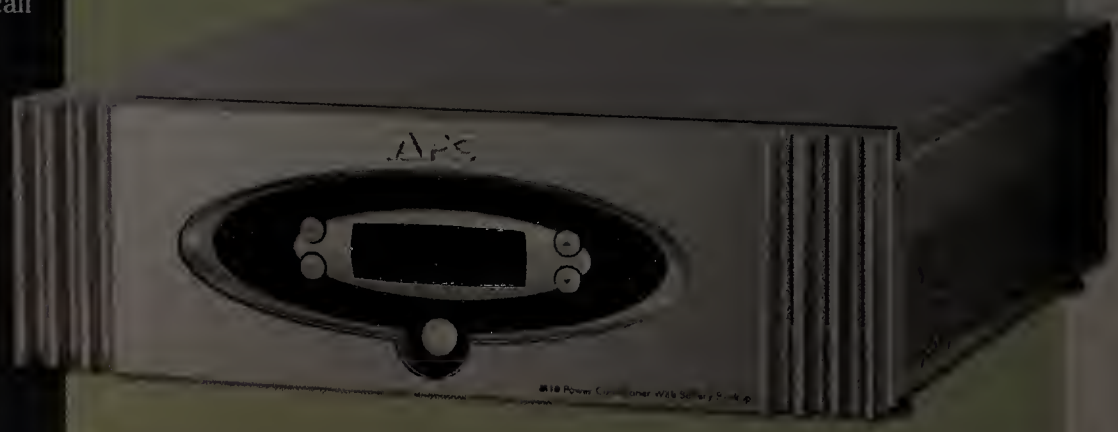
SECURITY BRIEFS

Mount Laurel, N.J., start-up Electronic Lifestyle Integration has shipped the first home network broadband security device to include managed services. The box, which costs $199, includes a built-in DSL router, four-port switch, 802.11g, USB port, USB printer port, VoIP port, phone jack, firewall and VPN. Plus, you get anti-virus, content filtering, anti-spam protection, monitoring and hardware replacement for $10 per month. Set it and forget it. **www.trusteli.com/consumers**

Mountain View, Calif., start-up GreenBorder introduced security software that isolates users' Internet activities from the desktop, then flushes all code, files and cookies when the user turns off the PC. The company says the technology lets you safely access any Web site, click any link, read any e-mail; and run applets or plug-ins without worry. Available now, GreenBorder will offer a free consumer version (that runs on XP Pro), and small-office and enterprise versions that include a server component that starts at $24.95. A Windows XP Home edition is in the works. **www.greenborder.com**

Send your users here for a short primer on wireless home network security: www.nwfusion.com, DOCFINDER: 6128

APC recently released new UPSs for home entertainment equipment. The PAC A/V H10 and H15 provide power conditioning, surge protection, noise filtering and voltage regulation to optimize a system's sound and video performance. Each features 12 surge-protected and filtered outlets, six of which include EMI/RFI noise filtering for digital devices such as HDTV monitors, digital video recorders, satellite dishes and DVD players. They also offer two analog, two video and two high-current (amplifier, subwoofer) filtered outlets. The H10 and H15 cost $300 and $400, respectively. **www.apc.com**



Buffalo Anywhere.

Access your PCs from anywhere with no monthly fee.

***NEW!* 125* High-Speed Mode™ Wireless Secure Remote Gateway –** WZR-RS-G54

Easy to configure VPN allows you to securely access and control your PC from anywhere in the world.

- One-Click Access to Network Services
- Complete Desktop Control of All Windows PCs
- No Monthly Fee – Free for Life
- Point-to-Point Access – No Middle Man Server in Place
- Secure File Sharing
- Stream Your Multimedia Content
- Remotely Turn On/Off Your Home or Office PC

nwl.buffalotech.com

* When operating in High Speed Mode™, this Wi-Fi device achieves an actual throughput of up to 34.1 Mbps, which is the equivalent throughput of a system following 802.11g protocols and operating at a signaling rate of 125 Mbps.

Out of the box

SimpleShare NAS just misses the mark

Lack of back-up software and high price hurts new network storage entry.

■ BY JAMES GASKIN

SimpleTech's foray into network storage is an almost-worthy introduction. The SimpleShare network-attached storage unit offers 160G ($399) or 250G bytes ($499) of space, but needs some minor changes, a price reduction and some extra software before it makes our wish list.

SimpleShare does some things very well. The unit, slightly larger and heavier than a VHS tape, is stylish and quiet. The case looks like it belongs on your media shelf next to audio components, and the near-silent operation won't distract.

Installation was pure plug and play, better than any NAS unit we've seen. The unit has been configured from the factory to scan the network and accept an IP address from any DHCP server. Other storage devices try to force themselves on the network and become the DHCP server, but this box plays well with others. Setup software from the CD finds the unit and starts basic configuration, primarily changing the administration password from the default. The client software then offers to assign the first open drive letter to the SimpleShare box, a friendly step we haven't seen before.

The SimpleShare administration utility requires ActiveX controls to run on the client, making Internet Explorer the only browser that interprets the screens accurately. Unfortunately, this runs counter to our advice to avoid Internet Explorer and ActiveX controls because of their susceptibility to spyware and viruses. (See "10 ways to stop spyware," page 16.)

SimpleShare includes a handy print server. Connecting a USB-only printer is easy, and the printer immediately appears on the network. But there are no print job controls — this might be acceptable for a home printer but not for a shared business device.

Linux users will be pleased — SimpleShare appears as both a Windows network resource and a mountable Network File System drive. Our Xandros Version 3 Deluxe Desktop happily printed through the SimpleShare using its Windows mode.

Now for SimpleTech's mistakes, which baffle us. These are all easy enough to fix and could make this a killer product.

First, at $499 for 250G bytes, SimpleShare is overpriced. SimpleTech's USB external hard disk drive, in the same case with the same specifications, costs less than $1 per gigabyte ($210 for 250G bytes). The cost of adding an Ethernet port and Web server software doesn't justify the price boost. SimpleTech has priced its NAS in line with competitors' devices, but those companies have a head start and brand recognition.

Second, SimpleShare lacks back-up software. For a home network or small office/home office (SOHO) NAS box, data protection must rank high on the features list. While the client setup disk maps a drive letter, it should then ask about data-protection measures, such as moving the default My Documents folder from a local PC to the SimpleShare, but it doesn't.

SimpleShare

Price: $399 (160G bytes), $499 (250G bytes).
Installation time: 15 minutes
Ongoing maintenance: Set and forget.

Bottom line: So close to an excellent NAS; lack of back-up software and aggressive pricing hurts it.

SimpleTech offers StorageSync Pro back-up software free on its Web site but only with its USB external drives. Modifying the software to work with only its own products would be better than nothing.

Some blank help system pages and poorly conceived administration pages also nagged us. It's great that SimpleShare uses fairly advanced drive pooling technology, but how many consumer and SOHO users understand drive pools?

SimpleShare does many things right, which makes the mistakes so painful. If the company addresses these issues, particularly the back-up software and pricing, we gladly would recommend it.

Gaskin can be reached at readers@gaskin.com.

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 36 WEST KINGSTON RI

POSTAGE WILL BE PAID BY ADDRESSEE

APC®

KEY CODE: y671y
Department: B
132 FAIRGROUNDS ROAD
PO BOX 278
WEST KINGSTON RI 02892-9920

When the power's on, you'll love it.
When the power's out, you'll love it more.

Introducing the New APC AV Power Conditioner with Battery Backup*

pure sine wave battery backup | surge protection | noise filtering | voltage regulation

Protect your investment, enhance system performance, and prevent interruptions with the only all-in-one unit on the market that defends against all power threats, including brownouts, and blackouts.

APC AV's pure sine wave battery backup power prevents lost pre-sets, missed DVR recordings, and lost or corrupted multimedia server data.

Additional battery packs are available to provide hours of battery runtime, while isolated noise filtering and voltage regulation eliminate bad power as a source of AV signal degradation.

For 20 years, APC has been a pioneer in new power protection technologies, resulting in countless industry awards, design patents, and tens of millions of units installed.

Get advanced power conditioning, surge protection, and battery backup from the APC power experts, and let the difference entertain you.

APC AV
ENGINEERED POWER SOLUTIONS℠

*Available December 2004

Engineered for high performance AV systems by the power experts

- Voltage regulation automatically corrects damaging low and high voltages
- EMI/RFI filter banks are isolated to prevent device noise from polluting other connected components
- 3 sequenced outlets prevent stress to speakers and help manage current draw on startup
- DC trigger enables remote sequenced turn on/off of 3 sequenced outlets
- Display panel and LEDs provide advanced monitoring and configuration
- Fan only operates when on battery or under extreme thermal conditions for sound control
- Battery backup output waveform is Pure Sine vs. the square wave found in inferior Uninterruptible Power Supplies (UPS)

CEDIA
CUSTOM ELECTRONIC DESIGN & INSTALLATION ASSOCIATION

Enter to WIN a FREE APC AV Power Conditioner with Battery Backup - $1499.99 ERP.
Visit *http://promo.apc.com* Enter Key Code y671y
Call 888-289-APCC x4292 Fax 401-788-2797

E-mail: esupport@apcc.com • 132 Fairgrounds Road, West Kingston, RI 02892 USA AV3B4EF-US

APC®
Legendary Reliability®

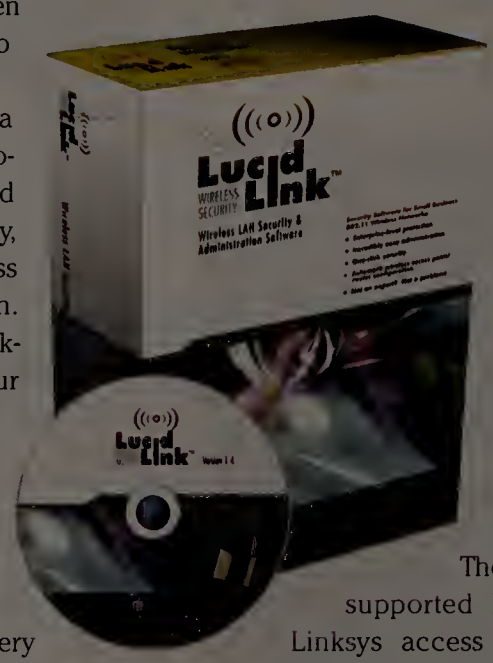
Strong wireless security for the SOHO network

LucidLink makes it easy to shut out unwelcome guests.

■ BY PAUL FERRILL

It's likely your home users haven't enabled security on their wireless networks. As the go-to guy, you can configure security settings for them and hope those users don't mess those settings up, or add software that lets users add and remove new and visiting users (as for when your teen's friends come over) without much effort (or calling you on the phone). That's the idea behind Interlink Networks' LucidLink, which provides enterprise-level wireless security simply enough to use on the home network.

The software uses encryption based on Wi-Fi Protected Access (WPA), along with advanced authentication techniques to protect network traffic and initial access. It uses a client/server model to authorize only those clients given specific permission to access the LAN.



WPA provides a higher level of protection than Wired Equivalent Privacy, but it doesn't address user authentication. Granting and revoking access to your wireless network, say, at the beginning and end of a LAN usage cycle, often involves changing the encryption key on every system on the network. LucidLink streamlines this process down to two button clicks.

The software also includes automatic access point configuration, but for only four devices from two vendors. We tested LucidLink Home Office Edition with a D-Link Systems DWL-2100PAP access point and DWL-G650 PC Card wireless adapter.

Setup includes installing server software, client software and an optional remote administration tool. The server requires a wired connection to the LAN via an access point or router, and a static IP address. The static IP tells the client software where to go for authentication. To test this, we configured the D-Link access point to use IP addresses 192.168.1.100 and above for DHCP and picked 192.168.1.40 for the server. We then installed the server software on a Gateway dual 3.06-GHz Xeon server with 2G bytes of RAM and running Windows Server 2003, although LucidLink also works on XP.

The server software includes a RADIUS server program that handles client authentication. After installation, a configuration application launches, which registers information such as access point hardware type and administrator password. You must choose either maximum security or maximum compatibility, and all clients connecting to one access point must use the same authentication/security settings. Maximum security is the best choice, but requires hardware that supports the full Temporal Key Integrity Protocol standard. The best option is to buy supported hardware such as a Linksys access point and a newer adapter card. LucidLink keeps an up-to-date list of compatible hardware on its Web site.

Client setup only took a few steps. We configured the wireless adapter first, forgetting to install the driver software before we inserted the card. Once we fixed that, the rest was a snap.

Next, we installed the LucidLink client software, which took only a minute or two. We created a user name and selected it. The administrator must authorize the user before he can access the network. The user guide includes a highlighted note recommending users shut down the system when changing users on an XP device to ensure a second user doesn't gain access to the network using the first's credentials.

LucidLink Home Office Edition

Price: Three-user, $99; 10-user, $499; 25-user, $895.

Installation time: Less than 30 minutes.

Ongoing maintenance: Each new user requires access rights to be granted, but this only takes a button-click. Backups of the configuration files also should be performed regularly.

Bottom line: Simple installation that hides the complexity of a RADIUS-based authentication server and 128-bit key security.

Access granted

Operation after this step is transparent. The first time a user connects with the LucidLink client, he has to wait until the administrator grants access from the "server" management console. Once approved, the client will connect automatically whenever it enters the access point's range. To connect to a different access point, you have to disable the client and re-enable the adapter to let Windows configure the wireless network settings. This could get to be a hassle if you switch networks frequently.

The LucidLink management console provides a simple interface. Users must be authorized for either a specific amount of time or granted unlimited access. Rescinding users' authorization is as easy as unchecking a box. However, when you revoke users' authorizations, they still have

access until they disconnect from the network. An event log also shows details for each authorization event.

The only administration task is backup and recovery. The manual recommends copying two binary configuration files to a back-up directory on another machine or external drive. Recovery consists of re-installing the software and copying the back-up files to a configuration directory.

Considering the work going on behind the scenes with RADIUS authentication and secure access key generation, the LucidLink software was pretty simple to install and configure. It was also easy to administer for a small number of users. For more than 100 users, the company offers an enterprise product.

Ferrill can be reached at paul@ferrill.net.

Netgear extends wireless reach with power-line technology

Good idea, but integration problems stopped us cold.

Wall-Plugged Wireless Range Extender Kit

Price: $149

Installation time: Between 30 minutes and two hours (depending on network).

Ongoing maintenance: Some maintenance required.

Bottom line: Don't try this unless you're on a homogeneous Netgear network.

■ **BY KEITH SHAW**

Even the smallest house can suffer dead spots on a wireless network because of obstacles such as building materials, wall mirrors and furniture placement. Meanwhile, power outlets live in abundance in most areas of the home, making HomePlug power line networking an attractive, although largely overlooked, alternative.

Netgear combined these two technologies with its 54M bit/sec Wall-Plugged Wireless Range Extender Kit, a two-device package that aims to fill wireless network gaps with power-line network connectivity. We tested the package to see whether it could enhance our wireless network and work with our network equipment.

The Netgear kit includes a power-line network bridge (left) and a wireless access point the plugs into a power outlet to extend one range of your wireless network.

The first device is a power-line adapter and bridge (model XE102), which plugs into a power outlet and connects to your router via Ethernet cable. The second device (WGX102) is the "wireless range extender," which plugs into an outlet in the dead spot area and acts as an access point.

Our first task was to find an appropriate dead spot. Our home is no mansion, and generally we've been getting good coverage. The access point sits on the first floor, so reaching up to the second floor and down to the basement isn't difficult.

Our basement still provided about 57% signal strength, which prompted us to do a little neighborhood war driving to find the outer edges of the current network. Not only did we discover that our network could reach a few neighbors' houses, but we also discovered that many neighbors are running unprotected networks without changing the Service Set Identifiers from the default setting.

Nevertheless, once plugged in, the second device (WGX102) is supposed to extend the range of the existing wireless network by providing additional wireless coverage. This sounds good in theory, but in practice we ran into several problems.

First, the Netgear device didn't play nicely with our Linksys router. Instead of providing a feature that would automatically grab an IP address from a DHCP server, it comes with a static IP address in a different range (Netgear uses 192.168.0.x; Linksys uses 192.168.1.x). To configure the wall-plug access point, we had to change the IP address on our wireless laptop to match the Netgear range.

Once we did that, we could configure the wall-plug adapter, but each setting change (such as adding wireless security) meant we had to re-associate with the access point each time. When we gave the access point a static IP address within the range of our Linksys router, the adapter still couldn't get an Internet connection. Checking the router, the IP address we had assigned the adapter didn't show up on its DHCP table; and because we had changed it from the original Netgear address, we now couldn't connect to the adapter to make any more changes. Luckily, Netgear adds a reset button on the wall adapter.

Which doesn't work, of course, so the adapter is somewhere in the IP address ether.

So if you want to extend the wireless range of an existing Netgear-based network, then this package might be worth a look. But if you want to integrate this with other equipment, pass on this and look instead for other ways to boost or extend the range. Just be sure to stick with the same vendor.

Shaw can be reached at kshaw@nww.com.

Keep

Best wa

Our go-to guys share

■ BY DEB RADCLIFF

It goes without saying, IT professionals know network security. In the orderly world of the enterprise, risks are assessed, strategies crafted and tools implemented. As important policies are created that users are mandated to follow, your mandates become company policy. Employees face consequences if they break network security rules.

Home networks are another story. The security risks are the same, but the tools are often limited and less mature. And the users? They span the spectrum: Some, like your elderly parents, just don't understand the risks and can be easily intimidated. Others, like corporate workers, are sharp but tend to get sloppy about security when IT's not watching. And kids? They're the worst; smart enough to disable your firewalls but most vulnerable to security risks and least likely to take them seriously.

Too bad you can't fire your teenager, or the CEO down the street for that matter.

So here's a security guide to keep in your toolbox — straight from go-to guys like you and others who deal with home users every day, either as their primary jobs or on the side. You'll also learn about new tools that ease network security and administration. (For more great security tips see "10 ways to stop spyware," page 16.)

Jeff Jorvig's u… understand why the anti-virus software they bought two years ago — and never updated — isn't protecting them.

HERE'S A TIP
Head online for security tip sheets and education resources.
www.networklifemag.com

Batten down the router

"Home network users don't even know they need a firewall, or the benefit of enabling encryption and MAC [media access control] address filtering on their wireless networks," says Jeff Jorvig, a home networking consultant in Chandler, Ariz. "But even I've got problems with my kids using Napster, Kazaa and LimeWire free music-sharing programs."

out!

ys to secure the home net

e tips for keeping home users safe.

Many go-to guys, Jorvig among them, feel a network-address translation router is sufficient firewall protection for the home — as long as administrative controls to add and delete programs are password-protected on each PC; and notebook PCs aren't moving in and out from public networks.

In both wired and wireless routers, the most important security step is to change the vendor-provided, default administrator password to a complex alphanumeric one. Some, like Scott Whitesell, of Believe IT in Battle Creek, Mich., take the additional step of keeping router passwords from their network owners. "It may seem kind of mean, but it falls into the category of what users don't know can't hurt them," he says.

But even with the most secure setup, routers can't protect themselves from users who open unsecured ports for gaming, let administrators in from their ISPs, or remotely log on to use tools such as GoToMyPC or PCAnywhere. And all too often, users forget to manually close these ports after using them, which makes them vulnerable to worms and hackers.

Enter PortMagic ($49), a router utility from Pure Networks that closes extraneous ports left open after usage. In April, Pure Networks will release Network Magic, a management tool that helps users develop a simple map of their network and offers alerts when unauthorized devices try to connect. Network Magic also provides alerts when router security is disabled and locks down file shares when a computer leaves the home network. The product runs on Windows machines but recognizes non-Windows connected devices.

Scott Whitesell's monthly newsletter alerts his users to software patches, viruses and frauds, and reminds them to run security scans and updates.

JENNIFER GIESEY

Wild wireless west

Jorvig, Whitesell and their brethren spend much of their time dealing with wireless networks. In fact, all the home LANs Jorvig served in the Phoenix area last year were wireless. Both go-to guys always turn off users' network Service Set Identifiers to hide the network from the outside world.

They also agree their biggest challenge is convincing users to turn on encryption. Even after Jorvig warns users of the risks, many still refuse to take the time to configure it. "There just hasn't been enough in the media to scare home users into believing they need it — yet," he says.

The good news is that setting up encryption is much easier on newer routers, including the Linksys Wireless G ($69) and SpeedBooster ($89) models, which encrypt to a user-created pass phrase for Wired Equivalent Privacy and Wi-Fi Protected Access. Next month, Linksys is scheduled to release push-button encryption on its routers, which synchronizes when you push a software button on a PC setup screen. Buffalo Technology's AOSS and WLAN chip maker Atheros' Jumpstart are similar. Of course, for these schemes to work, all your products need to use the same technology.

Although encryption is a good start, wireless networks need stronger protection, says Chris Basham, president of OTO Software, a Denver start-up. Basham argues that pass phrases can be guessed or cracked, and network MAC addresses travel unencrypted inside the network even with encryption turned on.

OTO's Wi-Fi Defense ($29) network utility automatically enables MAC address filtering so only assigned devices can connect to the network. (Currently, you need to enable MAC

address filtering manually on the router, which means inputting the IP address of each PC into the router interface.) OTO Software, like Pure Networks, works only with Windows PCs and supports only commonly used router brands.

Desktop defenders

Even with recent improvements, routers don't offer enough network protection, says Brian Milovich, a PC technician at a manufacturing firm in South Bend, Ind. Milovich also runs a small home-network consulting company with about 20 clients, most drawn from his circle of friends. File-share protection won't block worms and viruses when mobile computers connect to public access points.

"If your user gets his notebook infected on a public network and brings that infection home, it spreads through all those shared folders," Milovich says.

Routers do not block malicious code accidentally invited into the network by users who click malicious links and pop-ups, either. And a router can't prevent viruses and Trojans from entering PCs when PDAs, music storage or cell phones are connected via a USB port. Already, Trojan horses are spreading among Bluetooth wireless phones; it's only a matter of time before wireless worms and viruses try hopping between wireless networks.

So as an added layer of security, Milovich and Whitesell install software firewalls on their users' home PCs. Both prefer Zone Alarm's free product because it blocks outbound, malicious traffic. "I like to take my clients to a trash Web site and show them how Zone Alarm will freak out with all these alerts because it's blocking bad stuff," Milovich says.

But those same alarms can confuse users. "That's the hardest thing for them to grasp," Whitesell says. "A window popping up in what to them is Greek, saying 'this program is trying to access the Internet' could be an essential component of IE making a call. They tell it 'no,' and they've disabled it."

A good rule of thumb: "If an alert occurs when users are launching any kind of Internet action, such as connecting to their mail servers, downloading programs, connecting to a Web server, or updating software, then they should accept it," says Norman Merrell, a retired IT manager in Pennsburg, Pa., who administers the networks of his wife's home business and that of her cousin in Hawaii.

Tricks of the trade

Popular brands such as McAfee, Symantec and Trend Micro bundle firewall, anti-virus, spam protection, parental controls and security update services under one user-friendly setup. But users are still confused about updates and scans, which they must enable themselves.

"People think they're protected because they've installed anti-virus. They don't realize those definitions are two years old," Jorvig says.

Whitesell uses the free AVG anti-virus tool (www.nwfusion.com, DocFinder: 5853) and is testing Microsoft's new anti-virus/malicious software removal tool (DocFinder: 5851). He'll use it if it's offered free, provided it does a better job than the XP firewall. "Of course, it's hard to trust Microsoft with security," he adds.

Retired IT manager Norman Merrell supports the networks of his wife's home business and that of her cousin in Hawaii.

RICH DUNOFF

Another place to turn for free software might be users' ISPs. AOL 9.0 Security Edition includes McAfee VirusScan Online, McAfee Personal Firewall Express, and AOL Spyware Protection. EarthLink and Comcast offer similar services.

"One of my clients has PeoplePC as his ISP, which offers free firewall and anti-spyware protection," Milovich says. "It's a good added layer of protection, but I don't like it installed on work computers: That creates a headache for guys like me."

Workplace computers usually don't have software firewalls installed, so when his users bring their work machines home, Milovich installs Zone Alarm, as well as Firefox, which automatically blocks pop-ups by default.

Anti-spyware is most problematic for home users because the tools don't automatically scan, update or explain well what they find during scans. Milovich, Whitesell and Merrell each favor Ad-Aware and Spybot, which in conjunction net more spyware than others. And for free, the price is right.

"Once you get past the setup, Mom can run these," Milovich says. He and Whitesell put their users on an update schedule.

"I tell them when they get up on Saturday mornings to make coffee, run their spyware signature updates and scan their machines. It may take an hour, but they don't have to look at it," Milovich says. "Then I tell them to delete everything."

As technology evolves, vendors likely will meld anti-spyware with anti-virus signatures into one convenient scanner. Hopefully, we'll see point solutions such as Network Magic and Wi-Fi Defense cover all security problems in one package. But in the meantime, you'll have to kludge together what works best, and steep your users in ongoing education so they'll learn to be independent, Whitesell says.

"Education is everything," Merrell says. "People need to understand that their computers are a door to the world." ■

Get the Performance YOU Paid For!

Peak Performance!
Sharper, Crisper Video
Deeper, Fuller Audio
Longer Component Life Span

Tripp Lite has adapted its award-winning **isobar**® technology for the home/business theater market! Now you can enjoy:

Ultimate Protection
Superior surge-blocking architecture/highest joule ratings in their class provide the best protection available

Enhanced Audio/Video Performance
Exclusive line noise filtering technology delivers crystal clear signals

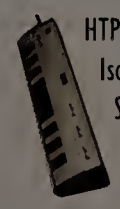
Continuous Viewing During Blackouts (UPS system only)
Battery backup support preserves recorder/receiver settings and programming

Protect Your Sound & Video Equipment With Tripp Lite Home/Business Theater Power Protection!

HT1500UPS UPS System

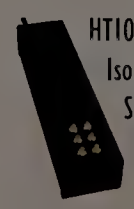
- 3 hr. runtime (recording)/15 min. runtime (viewing)*
- 8 outlets; 6 ft. cord
- 1-line coaxial (gold) surge protection
- 1-line tel/modem surge protection
- USB port; software for automatic PC receiver shutdown
- $100,000 Insurance

HTPOWERBAR10 Isobar® Surge Suppressor



- 10 outlets; 8 ft. cord
- 5700 joule rating
- Input voltage LED set
- Isolated Filter Banks; metal housing
- 3-line coaxial (gold) surge protection
- 1-line tel/modem surge protection
- $500,000 Insurance with Data Recovery Warranty

HT10DBS Isobar® Surge Suppressor

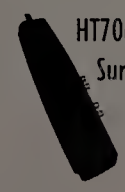


- 10 outlets; 8 ft. cord
- 3570 joule rating
- Isolated Filter Banks; metal housing
- 3-line coaxial (gold) surge protection
- 1-line tel/modem/ network and 1-line tel/modem surge protection
- $500,000 Insurance with Data Recovery Warranty

HT1010SAT3 Surge Suppressor

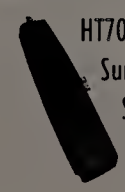
- 10 outlets; 10 ft. cord
- 3345 joule rating
- 3-line coaxial (gold) surge protection
- 1-line tel/modem/ network surge protection
- $250,000 Insurance with Data Recovery Warranty

HT706TSAT Surge Suppressor



- 7 outlets; 6 ft. cord
- 1680 joule rating
- 2-line coaxial surge protection
- 1-line tel/modem surge protection
- $100,000 Insurance

HT706TV Surge Suppressor



- 7 outlets; 6 ft. cord
- 1080 joule rating
- 1-line coaxial surge protection
- $50,000 Insurance

* Typical runtime based on VCR recording. Actual runtime may vary based on battery condition and load.

Win an HTPOWERBAR10 Home/Business Theater Surge Suppressor! $299.99 Value, MSRP
Register online at **www.tripplite.com/netlife** for your chance to win the ultimate home/business theater surge suppressor!
No purchase necessary. Valid through 4/30/05.

For more information, visit www.tripplite.com/hometheater

TRIPP·LITE
POWER PROTECTION

1111 W. 35th Street, Chicago, IL 60609
773.869.1234 • www.tripplite.com

10 ways to STOP spyware

Spyware cleaners fall short; follow these steps to stamp out spyware for good.

JAMES GASKIN

Sometimes the truth hurts, but here it is anyway: You will struggle with spyware at work, home, and on family and friends' computers for the next several years. Spam will be choked down to a manageable stream this year, but spyware will fill the gap, costing you precious hours cleaning the infected (and re-infected) computers of your friends and family.

My home office lab is the spyware front line. I routinely download programs for testing, then run a combination of pop-up blockers, spam protectors, Registry rooters and cookie cleaners. I'll quarantine 635 Registry spyware droppings one day, delete 31 spyware cookies the next and start all over again the next week. I've tested dozens of new utilities and dutifully download the latest version of each.

The bottom line is they're all good; they all help. But they're all incomplete. Running anti-spyware utilities is just part of the solution. There are a slew of other things you can do, and have your users do, to curb the problem. Follow our handy 10-step guide to get started.

1. Know thine enemy.

If you define spyware as any tiny cookie left behind by an innocent Web site, your frustration will never end. Scumware of all kinds will cause you grief, but the four major types are:

Spyware: an application surreptitiously gathering information about your computing habits that may send the data to some unknown site — aka "key loggers" or "keystroke capture parasites." (Not to be confused with "malware," which includes viruses, worms and Trojan horse programs.)

Adware: an application that pops up advertisement windows and banners randomly or based on current browser content — aka "pop-ups."

Hijackers: applications that change your browser home page, default search engine and even redirect you from sites you try to reach — aka "jackers" or "switchers."

Cookies: small files that track data such as Web site preferences and passwords for

NOAH JONES

repeat visits. Spyware gathers and spreads this information without user knowledge — aka "tracking cookies."

Adware is the most annoying, but hijackers and spyware do the most damage. Scumware purveyors claim we all "agree" to their garbage, but of course we don't. Yet, a lot of this stuff is harmless; teach your friends to tolerate a few cookies and save the 911 calls for aggressive pop-ups, browser home page redirects and suddenly sluggish systems.

2. Get off Internet Explorer

We can't charge Microsoft with a crime for creating spyware. But the design of Windows, and particularly Internet Explorer, certainly makes it an accessory. Encourage friends and family to switch to alternatives Firefox or Opera, which both block pop-ups by default. Firefox is free and available at (www.mozilla.org); Opera (.com) costs a few dollars.

Need proof Internet Explorer is the problem? On my primary test PC running Windows XP Home, I use Internet Explorer and Outlook Express. There were 739 spyware threats found. On my personal PC, running Firefox and Mozilla's Thunderbird e-mail application, there were 11 spyware instances. Each of those 11 was an Internet Explorer exploit or cookie that snuck in the few times I had to use Internet Explorer for certain Web sites.

But Microsoft is now making noise about anti-spyware tools (see "Giant Microsoft improvement?" next page), and XP Service Pack 2 has reduced the ability for most spyware to cripple a system completely.

Unfortunately, some sites demand Internet Explorer, and users who are heavily intertwined with Microsoft's Outlook e-mail client must use it. But there are ways to slow spyware using Internet Explorer. First, disable Microsoft ActiveX support. In Internet Explorer, click on Tools > Internet Options > Security > Custom Level, then click the check boxes that force ActiveX controls to ask permission before running.

Next, install the Google Toolbar, which also blocks pop-ups. It works on Internet Explorer 5.5 and higher, so you might have to upgrade the browser. Also, run pop-up blockers designed to work inside Internet Explorer, such as StopZilla, 123Ghosts Pop-up Killer, Ad Killer, Ad Muncher and Anti Popup Pro. (See sidebar for details, right.)

3. Deter downloads.

Walk this line carefully: Don't let friends and family — especially the tech neophytes like your grandmother — download anything. Then download and install the Google Toolbar for them. Explain why it's different from the weather station and smiley faces for their e-mails.

People want to download "free" programs from the Web, but teach them the difference between a site they visit for utilities (such as PCWorld.com or Tucows.com) vs. sites that appear in pop-up ads and spam.

Resolve not to get frustrated; accept that education will only work halfway. Spyware purveyors do a wonderful job convincing innocents to download spyware daily. Explain how what looks like a Google ad on the side of a browser page, or the link their good buddy sent them, is really a social engineering masterpiece of spyware diffusion. Sensitize your users to the most obvious danger signs, such as banner ads popping up offering a free spyware check (a cruel abuse of trust).

4. Teach back-up and restore basics.

Because many users won't heed your warnings, teach them how to recover from download disasters. People have too much on their computers today to resist back-up options. An external hard disk, tape system or CD writer full of back-up data can ease the sting of a spyware-ridden system and put things right with a restore to an earlier, spyware-free back-up point.

Teach users how to create restore points in XP and to set one before every download from a Web site that's not a brand-name portal. Disk space shouldn't be a problem on newer PCs, but even if they fill up their hard disks, eliminating some restore points is much easier than cleaning a spyware infection.

5. Create a spyware removal CD.

Remember your Boy Scout days and be prepared for the next call for help. Make your own spyware tool kit by burning a half-dozen spyware utilities to CD. When you go to clean a spyware machine, finding and waiting for utilities to download wastes time that's better spent with your own family. CD-ROM disks are inexpensive, so make extra copies and

SPYWARE HIT LIST

Utilities from trusted, name-brand portals are worth trying, if you're careful and back up before trying something new. These "usual suspects" appear in many downloadable sites. Try the freeware first and then commercial products in order of price, like this:

Ad-Aware SE Personal (free)
www.lavasoftusa.com/software/adaware/

Spybot Search & Destroy (free)
www.safer-networking.org/en/index.html

CounterSpy ($19.95)
www.sunbeltsoftware.com/product.cfm?id=410

Webroot Spy Sweeper ($29.95)
www.webroot.com

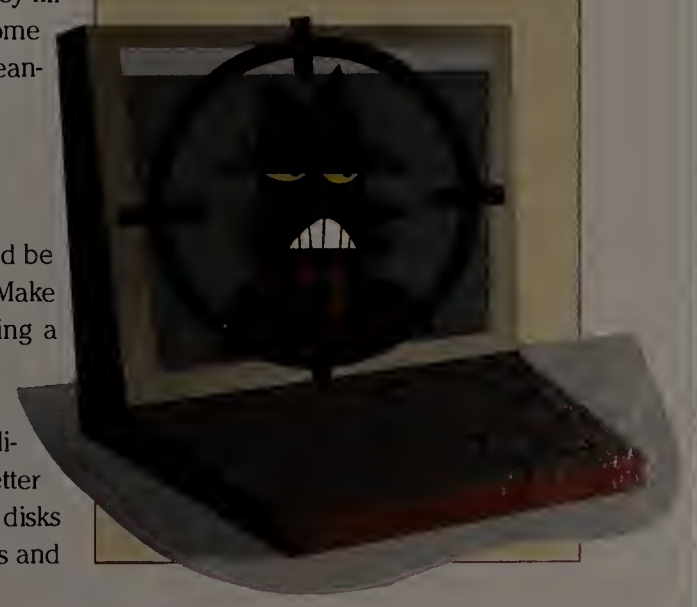
Intermute SpySubtract Pro (now includes CWShredder, $29.95)
www.intermute.com/products/spysubtract.html

PC Tools Spyware Doctor ($29.95)
www.pctools.com/spyware-doctor/

Pest Patrol ($37.99)
www.surfsecret.com/products/product-PESTP.html

SpywareKiller ($39.95)
www.spykiller.com

Xblock X-Cleaner Deluxe ($39.95)
www.securemost.com/antisp/x-cleaner.htm



give them to your users. On mine, I have three free utilities, with three trial versions of commercial utilities. The programs range from 2M to 10M bytes, so you'll have plenty of room on a standard CD.

6. Run at least two spyware cleaners.

You know from experience that no spyware cleaner even comes close to wiping every piece of malicious code. All utilities have blind spots that spyware programmers exploit. Every vendor says its product catches everything, but whenever I clean a hundred threats with one utility, a second always finds another dozen or so.

Every spyware cleaner checks the Registry, but because spyware follows Microsoft rules for Registry entries, nothing can clean it completely. Just when you think you have spyware beaten, the Task Manager process list will start to grow as spyware hiding in the Registry revive, especially after a reboot.

Run several utilities, run them regularly, vary them and make sure they're all up to date. Paid cleaners provide more constant signature file updates, but even freeware adds new capabilities regularly. Run, update, run, update, repeat. I clean a system, reboot into Safe Mode and clean it with a second tool, then reboot again.

7. Close desktop communication holes.

Every spyware upload means more future problems as spyware updates itself and adds new "features." Blocking the outgoing messages improves your users' quality of life.

Some, but not all, resident anti-spyware utilities block spyware uploads. Commercial products are a bit better. But installing a personal firewall also will block uploads. ZoneAlarm and Sygate Personal Firewall are both excellent.

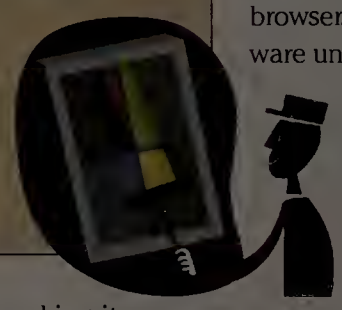
Nearly all name-brand routers sold today also include firewall protections. Look for products that do stateful packet inspection of incoming and outgoing packets. A combination of personal firewall and router controls isn't overkill, especially for users who can't resist the lure of spyware-laden sites.

8. Deal with DRM.

One reason spyware will be around for the next several years is that companies are increasing their use of digital rights management (DRM) on entertainment files and software authorization license files that let certain applications execute. The holes we leave open for these apps will be exploited by spyware for years. Tracking cookies, such as frequent buyer perks for online stores, make Web sites easier to use. The trouble is, they look just like spyware, making it hard to kill the bad files without killing the good files, too.

GIANT MICROSOFT IMPROVEMENT?

Giant AntiSpyware wasn't a big name until Microsoft purchased it. The Microsoft AntiSpyware Beta (www.microsoft.com/athome/security/spyware/software/default.mspx) is essentially the Giant AntiSpyware utility. Will Microsoft give the final version away free? We don't know. Will it roll the utility into a new security patch? It hasn't said. Waiting for Microsoft to fix spyware, however, reminds us of "Waiting for Godot."



The same is true for emerging entertainment player applications. The music files you download today and try to write to an MP3 player tomorrow will need to verify you have the right to play the files on that mobile device. Your new spyware protection software might block the DRM query to the authorization database. Isn't one definition of spyware an app that sends system information to a third party without permission? That definition applies to business application license files and DRM application licenses alike, at least on an application-interface level.

One answer is to avoid DRM applications such as music players, especially those from Microsoft. If you prefer your music, get a resident commercial spyware utility that updates its spyware database regularly because it will coordinate protection with the music services.

9. Leverage AOL membership.

Spyware protection from AOL, free for download for AOL members, is another useful addition from AOL as it continues to regain relevance. I found scanning speed to be slower than many other spyware cleaners, but the program found seven additional spyware instances after CounterSpy and SpyBot were through.

AOL offers some valuable protections for families, such as parental controls, but its browser is based on Internet Explorer and therefore suspect. At least AOL helps its members with toll-free tech support for times you're unavailable.

10. Recommend a Macintosh or Linux system.

Spyware attacks Microsoft operating systems primarily, entering through Internet Explorer holes and hiding inside Windows weak points. Some spyware, especially malicious cookies, functions within any browser, but that's a tiny fraction of the spyware universe.

Microsoft applications such as Internet Explorer, Word, Outlook and Media Player execute applications automatically when downloaded, allowing spyware easy access. Linux and Mac operating systems don't allow this automatic execution, making them more spyware resistant. Worse, Windows lets any user (or spyware) load dynamic link libraries into the kernel, while administrator privileges for Linux are required for that level of system access.

Is the hassle of changing a friend's operating system or entire computer worth avoiding the hassle of spyware? Not to most people, but Apple and Linux will welcome you if spyware becomes too painful.

Because you're carrying a CD full of anti-spyware utilities already, throw in a CD of the Knoppix bootable Linux OS (www.knoppix.com). Use it to verify badly infected systems still function booting and examining the system, and let your family and friends see how Windows-like modern Linux has become.

Gaskin has been helping small and mid-size businesses use technology intelligently since 1986. He can be reached at readers @gaskin.com.

PROTECT YOUR CUSTOMERS FROM THEMSELVES.

Your customers are curious people. They surf the web blindly, open e-mails unwittingly, download without discretion, and are baffled when their PCs go down. After bravely attempting to solve things on their own, they finally come to you with a seriously compromised system.

Webroot has developed **System Analyzer** to help you quickly identify and remedy system problems and insulate your customers from further risk. Webroot System Analyzer comprehensively diagnoses a PC's security flaws, infection rate, and performance problems, and generates a recommendation report for your customers.

webroot®
SOFTWARE, INC.

The creators of the award-winning Spy Sweeper™

FREE | Webroot System Analyzer. Get yours FREE at www.webroot.com/shockme

Security chief

Phishers use spears, hooks and nets

How to protect your users from insidious attacks.

Most of your friends and families have heard about phishing. They might even know enough to ignore e-mails claiming a problem with their accounts, even to check the URL of sites they're not sure about.

Unfortunately, phishers have raised the bar — and now are using spyware to load keystroke loggers to capture users' banking information.

In January, the Anti-Phishing Working Group identified a Brazilian phish site selling Visa cards that loaded a program called visa.exe onto the end user's directory. Upon reboot, the application modified system registry files and logged keystrokes when predetermined sites were accessed, and then sent that information back to the attackers. Dave Jevans, the group's founder, says phishers can use the same techniques to install hijackware. So when users type in Citi.com, they're redirected to a password-harvesting site that looks just like a Citibank site.

Until recently, the bad guys had to attack browser vulnerabilities to trick the browser into giving what looks like a legitimate URL. But now a new Internet Corporation for Assigned Names and Numbers (ICANN) standard makes browsers vulnerable to spoofing without hacking. ICANN approved the use of international characters in international top-level domains, which paved the way for the new International Domain Names (IDN) standard to add thousands of new character types. Phishers use some of these character types in place of English-language characters to make fake URLs look real.

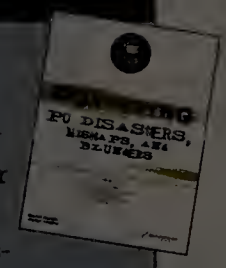
In February, Secunia, a Danish security company, posted information about the IDN vulnerability on its Web site. At the time, Firefox, Opera, Safari, Omniweb, Netscape and Conqueror browsers were vulnerable to IDN spoofing. If Microsoft adopts the use of IDN, Internet Explorer will be vulnerable, too.

We tested Firefox and Safari against a test developed by security expert Eric Johansen (see www.nwfusion.com, DocFinder: 6422). When both browsers displayed a perfect spoof of paypal.com, I fired off an e-mail to Secunia asking: "Why haven't browser vendors done anything to reverse this?"

Secunia's CTO Thomas Kristensen replied with a question of his own: "Who should you blame — ICANN, the browser vendors or other parties who wanted to implement special national characters without listening to criticism that [goes back to] 2002?" Kristensen says the browser vendors should take responsibility and reverse their support for IDNs.

Radcliff is a California writer specializing in online safety and network security. She can be reached at www.deb.radcliff.com.

SECURITY TOOLBOX



Good book

Surviving PC Disasters, Mishaps and Blunders by Jesse M. Torres and Peter Sideris covers everything from operating system failure, to lost MP3 files, to lost or stolen equipment, with a strong chapter on backup and recovery.

Tales from the front

We'd love to hear what home network security issues you face — and how you deal with them. Write to securitychief@nww.com.

HOW TO DODGE THE HOOK

Experts predict phishing attacks will get more prolific, complex and organized over the next two years. Install pop-up blockers, switch to a secure browser such as Firefox (or at least patch Internet Explorer regularly), and use multiple spyware tools. Send users to see Microsoft's phishing video: www.nwfusion.com, DocFinder: 6423. Look to Phishing.net for no-cost toolbars that identify known phish sites. FraudEliminator (www.fraudeliminator.com), a free, stand-alone browser plug-in to Internet Explorer, provides a site status button beneath the URL (green, yellow and red), control over pop-ups and reporting. The trouble is, such toolbars rely on a database of known phish sites, which come and go in hours or days. Look for multi-factor authentication services: AOL offers RSA Security tokens for $10 each and $2 to $5 per month. Banks are adopting an authentication scheme from Strikeforce that calls users' phones and prompts them for their PIN. LyfeCards is promoting this to 50,000 retail merchants. See a demo at DocFinder: 6424.

Tech spy

HomePlug charges up

Powerline is poised to deliver both whole home networking and broadband services.

If you judge a home network technology's success by its retail presence, then HomePlug is dead. Linksys, Netgear and others still sell HomePlug 1.0 LAN kits, but sales languish in the low single digits.

For a time, HomePlug seemed like a smart way to boost spotty coverage on a wireless network, and Netgear recently shipped a hybrid HomePlug/802.11g kit. But now that the new wave of g-MIMO gear boosts wireless coverage so well, who needs it?

We do, really. Although HomePlug began life in retail products, its future is in embedded technology — in routers, notebooks, and thermostats, in TVs, DVRs and music players. The upcoming DOCSIS residential gateway design calls for both HomePlug and 802.11 to be built in, for instance.

The HomePlug Powerline Alliance has big names sitting on the board: Comcast, Sharp, RadioShack and EarthLink. New board members include EchoStar, Leviton, Duke Power and Sony. Yes, Sony.

So what are these guys banking on? HomePlug AV. HomePlug Broadband over Powerline. Home control.

When the HomePlug AV specification is ratified in June, HomePlug will deliver a 200M bit/sec data rate, with expected throughput just shy of 100M bit/sec, which makes it ideal to transmit multiple streams of video throughout the home.

Intellon today has 98% of the HomePlug 1.0 market for silicon, but Arkados and Conexant Systems plan to build HomePlug AV chips, with others like Broadcom expected to join the market. The first HomePlug AV products should ship around October, and you should recommend them. Overall, HomePlug gear is reliable, secure (encryption is built in) and toaster-easy to set up.

As significant, the Alliance chose the HomePlug AV specification as the basis for its upcoming HomePlug Broadband over Powerline (BPL) standard, expected to be ratified by year-end. This means in time you'll be able to buy broadband equipment and services from your power supplier that work seamlessly with your HomePlug LAN equipment. Moreover, BPL means increased broadband access for rural communities, and improved energy management and efficiency.

Say you have a HomePlug AV HDTV and get broadband service and IPTV from your power utility provider. You'd be able to access the Web from your TV and retrieve content without a set-top box, computer or any other device — straight through the power lines. Then envision adding other applications such as HVAC, security systems and VoIP phones.

There's only one problem. Two competing groups recently formed with plans to develop their own power-line network technology, which competes directly with HomePlug.

The United Powerline Association includes DS2, iLevo, Ascom, Ambient and Corinex Communications. The other is CE-Powerline Communications Alliance, whose members include Panasonic, Mitsubishi and Sony. (Yes, Sony joined both this and the HomePlug Powerline Alliance.)

If you buy HomePlug AV gear for your house, but your utility provider ends up offering services based on DS2 technology, they won't work together.

Lastly, the HomePlug Alliance just announced it would develop a low-power, low-speed power-line network protocol, an alternative to proprietary technologies including x-10, HaVI, Echelon LonWorks — for controlling lighting, blinds, garage door openers and the like. Vendors should begin proposing technologies this month, with testing to begin in April. It's too early to say whether the technology will interoperate or merely coexist with HomePlug, though. ■

SPY REPORTS

Actually, **broadband over power lines** arrived in 2004, with more than 20 pilots and commercial deployments using proprietary technology. More than 250,000 U.S. households already have the BPL option — according to a report from the New Millennium Research Council — including parts of New York City through Ambient and all of Manassas, Va., through COMTek.
www.thenmrc.org/archive/bpl_report022405.pdf

Home control vendors including Leviton and Intermatic recently formed the **Z-Wave Alliance,** an industry consortium of companies that build wireless home control products built on Zensys wireless mesh technology. Z-Wave lets you monitor and manage lighting, security systems, thermostats, garage door openers, entertainment systems and other devices. More than 75 Z-Wave products have shipped already, with an additional 100 expected by summer. In a Z-Wave home, you can program the lights to go on when the garage door opens; the blinds draw and the lights dim when the TV comes on. You can program devices remotely, turning the thermostat up on the drive home from work. Soon we'll see Z-Wave built into routers, and Ethernet to Z-Wave bridges.
www.zwaveallliance.com

Connection coach

Secret phone calls and security snafus

Sibling rivalry meets the home network.

All this talk about spyware and phishers bringing you down? Learn what to do when security, misapplied, kills your computer and inexpensive ways to play spymaster with encrypted voice calls.

Marie from Atlanta: Our older daughter wants to keep her little sister from listening to her phone conversations. Does VoIP provide encryption to keep conversations secret?

Coach: VoIP providers like Vonage and AT&T CallVantage don't, no. But remember, conversations have to connect to traditional telephone lines to reach people who aren't using VoIP, so any encryption would have to be decoded at the VoIP-landline connection point, anyway. Besides, providers eventually will fall under the federal wiretap access laws, making encryption a no-no.

But Skype Technologies, which lets you make free voice calls between PCs, encrypts voice connections. Your older daughter and up to 50 of her paranoid co-conspirators will need a headset to connect to their PCs, but once they download the Skype client software, they can talk over 256-bit encrypted connections.

Phil from outside Chicago: I recommended my neighbors sign up for VoIP, but now they're mad because none of their extensions work.

Coach: The easiest way to regain the convenience of extensions is to buy new cordless phones that are "expandable" and support multiple handsets from vendors such as Motorola, Panasonic, General Electric, AT&T, Uniden and others.

Some support up to eight handsets. Office warehouse stores and online retailers have models you can buy with two handsets for about $100. Extension handsets tend to be in the $40 to $50 range each.

Readers in the Northeast have another option — Optimum Voice. Owned by Cablevision, Optimum Voice installs the broadband phone router at the telephone company demarcation point. This runs the broadband phone connection over the installed home phone wiring by plugging the start of the house phone wiring into the VoIP router or telephone adapter, so your extensions work.

If you can get it, Optimum Voice charges a premium over other VoIP providers ($40 vs. $20 to $25), and installation requires a truck roll and technician time.

If you can get to your demarcation point — usually a gray box on the side of the garage where the phone line connects — you can do the same thing by following the instructions on the Vonage Web site wiring help pages. But beware: If you keep a traditional landline, doing this will disable it.

Connor from San Diego: My son set the BIOS password on our family desktop to keep his sister from using it. He doesn't remember the password, or he mistyped it initially. Now we're locked out of the computer. Help!

Coach: Another overzealous security sibling? Just be glad he didn't do this to your laptop. Security chips in many laptops make recovery from a lost BIOS password difficult and expensive.

Most desktop computer motherboards have a jumper labeled something like Clear CMOS, Clear Password, PASSWD or CLRPWD. Look along the edges of the motherboard near the CMOS battery (the quarter-sized disk on the motherboard). Change the setting by removing the black jumper covering two pins, or moving the jumper from pins 1-2 to pins 2-3. Then restart the computer, reset your password and change the jumper setting back to the original setting. If that doesn't work, take the CMOS battery out for 10 minutes, and that should reset your password. This also will reset everything else configured in your motherboard, all of which will have to be supplied by you or re-discovered by the system upon reboot.

Another option is to try the backdoor passwords that BIOS vendors program into their chips. Call support for help, and be careful. Some BIOS routines will lock you out after three wrong password attempts. (On a business computer, you can pull the hard drive and put it into another system to read the data, because the BIOS password doesn't involve the drives.)

For a list of generic passwords, head to www.nwfusion.com, DocFinder: 6421.

If you do have this problem with a laptop, check out Password Crackers at www.pwcrack.com and buy a replacement security chip for your laptop.

Send stumpers to connectioncoach@nww.com.

COACHING TIP

Spring cleaning applies to security, too. Remind family and friends to go through their e-mail, online banking, and other Web site passwords and change them. Those with wireless routers should watch out for unknown computers (DEN-PC? We don't have a den . . .) showing up in the "Connected Systems" page. If one does, tighten your wireless security settings.

Off the clock

Sonos: My kind of network music system

This Digital Music System knows and loves networks.

Sonos certainly isn't the first company to have a networked digital music player, but it's the first one to understand networking.

This became obvious when I loaded the software on a PC and it gave me the option to play music stored on a network share — in my case, a LinkStation network-attached storage (NAS) device from Buffalo Technology. Other systems might let you play music off a NAS, but only the Sonos Digital Music System lets you do it so elegantly.

Elegance is the name of the game for the Sonos system, from its shoe box-sized ZonePlayers, to its sleek ZoneController two-handed remote control with color LCD screen that lets you play different songs in different rooms, or the same music in every room simultaneously.

The second indication I was in friendly network territory was when the instructions recommended a router. Every other system takes the lowest common denominator route, by assuming you have only one computer.

Installation of a ZonePlayer involved connecting two speakers, plugging the Ethernet cable into the router, and plugging in a power cord. After that, a quick software install onto a PC got us up and running. You don't have to install the software. Instead, you set up everything through the remote control. However, using the software was easier than running through the ZoneController menus.

Only one ZonePlayer needs to connect to the router. More ZonePlayers will communicate with it via a proprietary wireless mesh network (2.4GHz). But they need to plug into a power outlet.

With everything installed in less than 15 minutes, you'll spend the rest of the time learning the intricacies of the ZoneController remote control and the DesktopController software. Depending on the number of ZonePlayers installed, you can use either the remote or the PC software to pick which songs to play in which zones. Playing a song or switching zones was instantaneous. We experienced no delays any time we switched.

As a bonus, Sonos bundles many Internet radio stations. After a bit of searching, I easily added several streaming radio stations to the system.

My only gripe with the system was its method of loading songs to play: The software requires you to create a queue (playlist) of individual songs. When you select an album with the Sonos system, it only plays the first song unless you queue up the entire album manually.

The other potential stumbling block is price. A starter kit with two ZonePlayers and the ZoneController costs $1,200, and extra ZonePlayers cost $499. Speakers are extra (Sonos provided us with two sets of $150 speakers, but you could use your own). Once you get hooked, you'll want to outfit several rooms with ZonePlayers, which could ring up a hefty bill. ■

Digital music has a new standard with the Sonos system.

OFFLINE PURSUITS

All-in-one photo lab

Epson's Stylus Photo RX620 is a photo printer and scanner that can restore colors to old photos, slides or negatives. It supports 11 types of memory cards and can print a 4-by 6-inch photo in 39 seconds. The RX620 costs $300.

Street soccer strikes

Look, ma: No hands!

First there was street-style basketball, then football — now comes world football. Electronic Arts' EA Sports BIG division has shipped FIFA Street, an arcade-action soccer game that lets you play four-on-four soccer in various street locations. The $40 game is available for Playstation 2, Xbox and Nintendo Gamecube.

LINKSYS®
A Division of Cisco Systems, Inc.

WIRELESS MEDIA EXTENDER

Enjoy digital media from the comfort of your favorite room!

The new Linksys Media Center Extender connects a Media Center PC with a TV and stereo system anywhere in your home. Enjoy digitally recorded TV shows without commercials! Watch downloaded premium movies, listen to your MP3s, or view digital photos from the comfort of your living room. Even chat on-line with your friends while watching TV!

Designed for Microsoft® Windows®XP Media Center Edition

WMCE54AG
Dual-Band Wireless A/G Media Center Extender

BEST BUY
Thousands of Possibilities GET YOURS™

Visit www.Linksys.com today for product details, or call our Advice Line at:
1-800-737-7201

CISCO SYSTEMS

A Heartbeat Away

Network Life Line

A new e-mail newsletter for the home network go-to-guy from the editors of *Network Life.*

Register for the Network Life Line Newsletter and be entered to win!

Grand Prize:
23" Sony LCD WEGA™ Flat Panel TV

Second Prize:
One of 5 4GB iPod Minis

Go to www.networklifemag.com/sweepstakes to sign up today.

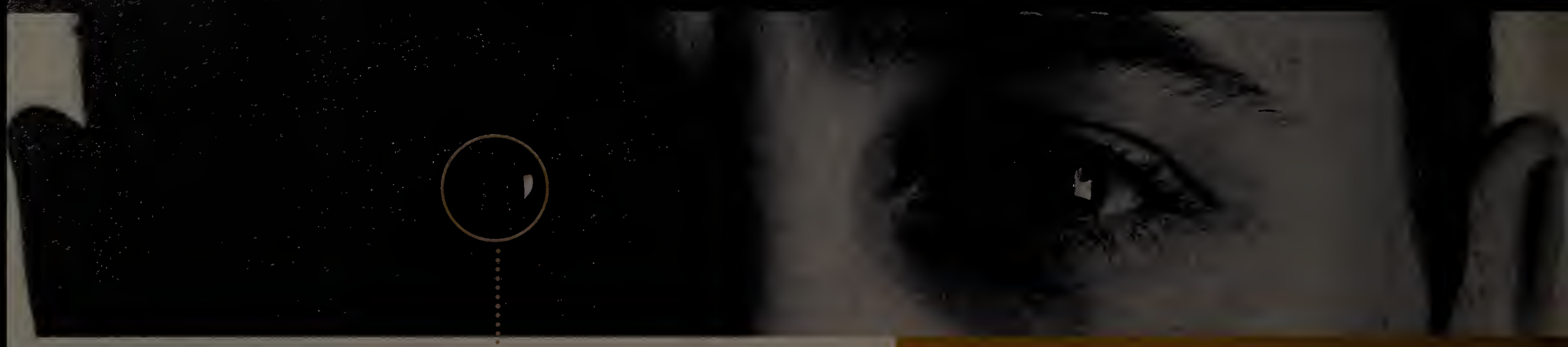
Network Life Line — an alert-based e-mail newsletter that will keep you informed about exciting new content on the Network Life Web site (www.networklifemag.com) — the expert's guide to the connected home.

Register today at
www.networklifemag.com/sweepstakes

NetworkLife™
THE EXPERT'S GUIDE TO THE CONNECTED HOME

Complete sweepstakes rules are available at www.nww.com/nwliferules.pdf. Offer expires June 1, 2005.

Controlling outcomes is just a matter of wired and wireless Network SuperVision™ with one integrated tool



OptiView Series II™
Integrated Network Analyzer

Our new OptiView Series II Integrated Network Analyzer shows you more of what's happening on your network than you may have ever seen before. And faster. The graphic user interface and information-rich front page shows what's happening everywhere on your network in seconds flat – even on wireless LANs and VLAN segments. Analyze 802.11 a/b/g WLANs just like you analyze your wires. That's troubleshooting with super vision. But it's not all. OptiView also gives you powerful monitoring and analysis capabilities to optimize your network performance. In fact, it's the world's only integrated tool that combines all three – troubleshooting, monitoring and analysis capabilities – into a single portable unit.

Seeing is believing. Go to www.flukenetworks.com/optiviewdemo and imagine the awesome control it puts in your hands.

FLUKE networks

NETWORK SUPER VISION™

Enterprise Computing

■ WINDOWS ■ LINUX ■ SERVERS
■ STORAGE ■ GRID/UTILITY ■ MOBILE COMPUTING

Going fault-tolerant for less

■ BY JENNIFER MEARS AND DENI CONNOR

At the Boston Stock Exchange, the ability to get traders the market data they need is critical. So when it came time to replace the Exchange's fault-tolerant system that supported its ticker-processing application, the project wasn't taken lightly.

Instead of upgrading on the proprietary Stratus Continuum platform that the application had run on for more than a decade, IT executives at the Exchange decided to try something new: They stuck with Stratus but brought in one of the vendor's lower-cost, Intel-based systems running Linux.

"For cost purposes, we switched to the ftServer," says Tom Targonski, vice president of the project management office at the Boston Stock Exchange. "The reliability was there, the scalability was there, and the performance was there."

At the same time, the cost savings — compared with running one of Stratus' proprietary machines — are expected to be significant, Targonski says. While he wouldn't cite specific figures, Targonski says the savings will come from lower upfront and maintenance costs for the hardware, and reduced operating system licensing fees with Linux.

For some IT managers, it might come as a surprise that Intel-based, fault-tolerant systems running Windows or Linux provide the same — or better — performance than bigger, more costly boxes. In fact, in the past year or so, high-availability systems, once confined primarily to telecom and financial industries and costing millions of dollars, are becoming more affordable.

Fault-tolerant servers are specially designed with multiple system components that operate in lockstep so that if one fails, another picks up and the system keeps running. High-end systems such as HP's NonStop servers are massively parallel, running two copies of every job performed on the server.

In the past, such servers were strictly based on proprietary hardware. But more recently, industry-standard components are being used to build them. Stratus and NEC, for instance, offer Xeon-based fault-tolerant servers running Windows and Linux. HP, meanwhile, is migrating its NonStop line to Itanium.

"Industry-standard components with an operating system such as Windows or Linux have reached the point where you can configure a fault-tolerant system that is good enough to compete against [one with] proprietary components," says Vernon Turner, an analyst at IDC.

What that means for end users is a highly available server without the high price tag.

An ftServer T30 like the one the Boston Stock Exchange is deploying, for example, starts at about $30,000. In contrast, a comparable Continuum server, based on HP's PA-RISC chip and running Stratus' proprietary VOS operating system, starts at roughly $175,000.

. "And these [Intel-based] machines are smaller, so heating, cooling and power are less of an issue, and they're getting higher performance than we've had in the PA-RISC VOS platforms," says Denny Lane, director of product marketing for Stratus.

Because software must be tuned to run on the fault-tolerant architecture, Stratus enhances the operating systems delivered with its boxes. Stratus enhances Windows, but makes no change to the base code. However, it does provide its own fault-tolerant distribution of Linux based on the 2.4 kernel. Stratus has been working with the

See Fault-tolerant, page 26

Fault lines

Benefits and disadvantages of moving to Intel-based fault-tolerant systems:

Pros	Cons
Hardening things: Give Windows- and Linux-based applications a more reliable platform.	**Consider the source:** Windows- and Linux-based applications must be tuned for the new platform.
Falling prices: Provide an economical option at the high end.	**Cost analysis:** Typically, the cost will be higher than Intel-based clusters.
Manageable: Offer high availability, but without the management demands of a cluster.	**Being appropriate:** They aren't right for all applications.

Short Takes

■ **Symbian** has licensed a protocol from **Microsoft** to let users of mobile phones based on the Symbian operating system synchronize e-mail and other personal data with servers running Exchange Server 2003. Symbian plans to develop software based on Exchange Server's ActiveSync protocol for synchronizing e-mail, calendar, contacts and other personal information management data, and will make the software available to handset makers for use in future Symbian-based smart phones. Symbian didn't specify a timeframe, but said on past experience it should take about a year to release software. The licensing agreement follows a similar deal announced by Nokia — the primary seller of devices using the Symbian OS — and Microsoft.

■ **Microsoft** last week introduced a slew of partners that will develop supporting products for its **Network Access Protection** technologies. NAP is a set of technologies for evaluating desktop computers for security compliance before letting them on the network. Microsoft already has delayed NAP once and now says it plans to ship it in 2007. New to the NAP fold are AppSense, which will provide protection against unauthorized applications and malware; Aruba Wireless Networks, which will support wireless intrusion protection, user mobility and bandwidth management; and Bluesocket, which will offer wireless LAN security and management appliances and intrusion-protection technology.

HP preps blades for SMBs

■ BY JENNIFER MEARS

HP last week announced it is expanding its Smart Office initiative, launched two years ago to help small and midsize business get the most out of their IT resources, with a program focusing on blade servers.

Blades for Business is aimed at helping SMBs understand how the compact systems can fit into their IT strategy. The program is launching May 2 and will include information and resources on the HP Small Business Web site, consulting and integration services, and a new 1U power supply for a single HP BladeSystem chassis that is designed specifically for smaller implementations.

"It will bring down the price point and ease of deployment for [SMBs]," says Paul Miller, vice president of ProLiant and blade systems at HP.

SMB customers will be able to choose from HP's entire blade portfolio, including Intel- and Advanced Micro Devices-based systems. By packaging the blades with the 1U power supply, as opposed to the current 3U power package, customers will see savings in deploying as few as four blade servers, Miller says.

Today, customers need to deploy between six and eight blades to see cost benefits as opposed to traditional rack-mount systems, he says.

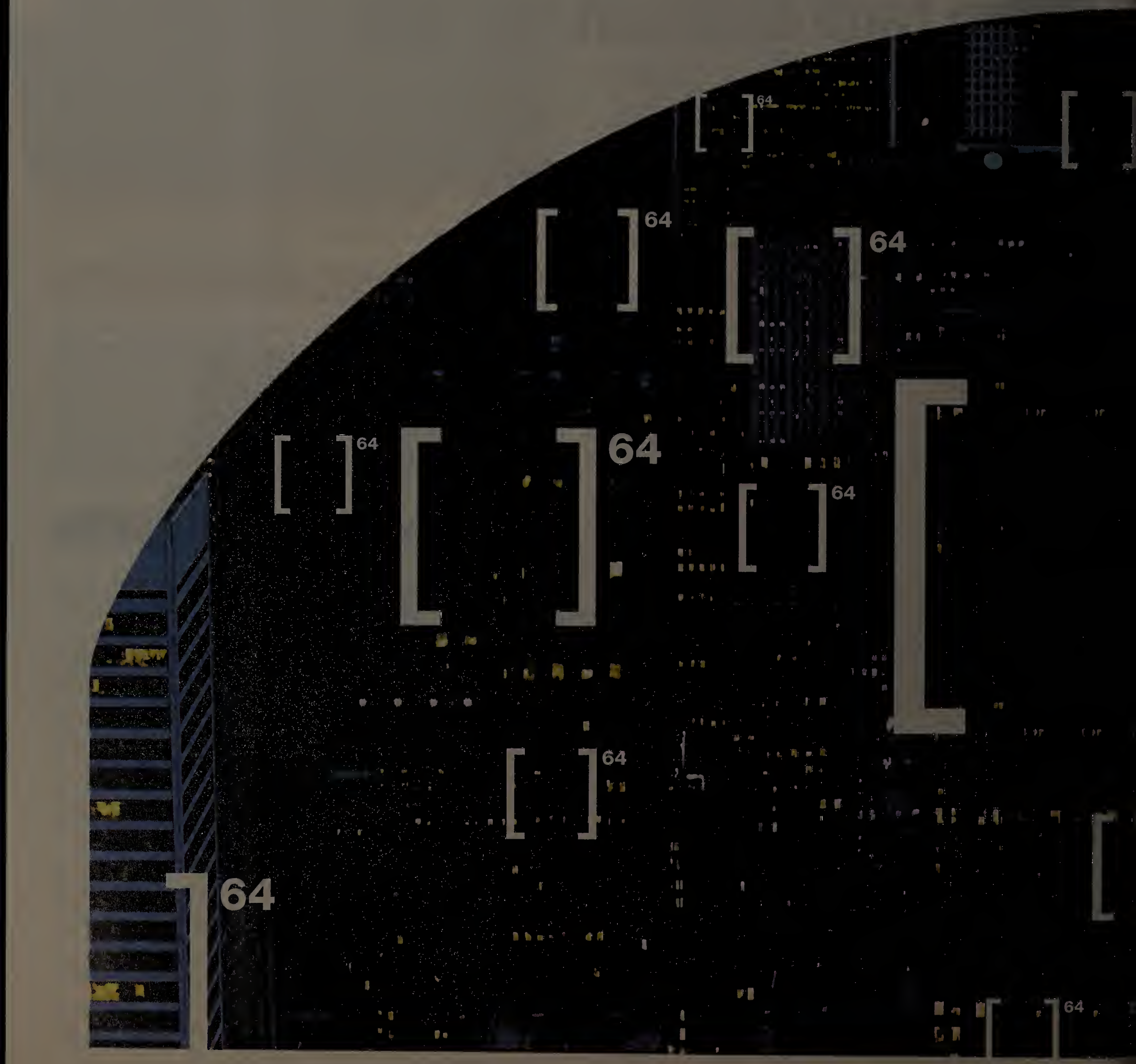
"Our [SMB] customers are asking for blades," says Vince Gayman, director of worldwide SMB product programs at HP. "A lot of the features and functions we emphasize for data centers aren't really what they're looking for. They're looking for simplification in a rack, a way out of the cabling mess and an easier way to manage their server environment. These are the fundamental things blades let them do."

With Blades For Business, HP is playing catch-up with IBM, which in October rolled out a BladeCenter chassis designed to lower the cost and ease deployment of blade servers for SMBs. The SMB-focused BladeCenter offering includes "business in a box" features aimed at simplifying the deployment of blades in Linux and Windows environments.

The blade market is growing fast, and IDC expects it to account for nearly $9 billion in server sales by 2008.

SMBs account for a large part of that growth, Miller says. HP already sells more than 40% of its blade servers into that market, he says.

Pricing has not yet been released. ■



Special Focus

STORAGE: Virtual tape libraries.

Taking the best of tape and disk

■ BY DENI CONNOR

Despite its relatively slow speed and overall bulkiness, tape has its strengths. After all, it's inexpensive compared with most disks, it's portable and has been used in data centers for years.

Still, traditional tape back-up systems have begun to wear out their welcomes at some companies, which are turning to virtual tape technologies.

Virtual tape — or tape emulation — combines traditional backup methodology with inexpensive disk drive technology to create a disk-based library that acts as a tape library. In concert with traditional back-up software from vendors such as Commvault, Legato Systems and Veritas Software, virtual tape products write data to disk in current tape formats. Because disk is used rather than tape, data can be backed up at channel speeds many times faster than with tape and also recovered more quickly. With this technology, IT staff no longer needs to mount, position and dismount tapes or worry about the reliability of the media.

As an IT executive at e-commerce and payment services vendor FirstData, Todd Cushing had no illusions about his company's data storage needs lessening any time soon. Neither did he think that the Omaha, Neb., company's current tape-based storage system was the answer.

FirstData turned to virtual tape technology, replacing 74 tape silos and 1,500 tape drives with seven virtual tape storage systems to back up 60T bytes of data on nine mainframes. FirstData uses StorageTek's Virtual Storage Manager appliances, which compete in an increasingly crowded market against products from established players such as EMC and Quantum and newcomers such as Diligent and Sepaton.

"Using [virtual tape libraries] rather than tape has saved us thousands of square feet in our data centers," Cushing says.

FirstData had been doing a lot of what Cushing calls "tape stacking." In other words, it had been converting oodles of tapes from one format to a common format to replace aging media and bring consistency to the operation. The process proved labor-intensive and was prone to errors, he says.

> **"We wanted to get these islands of backup under one enterprise product."**
>
> **Andrew Ferguson**
> Manager of enterprise operations, Brookhaven National Laboratories

Cushing says FirstData is mulling whether to use virtual tape technology for its Unix and Windows NT systems as well, which require about 12T bytes of data backup. While these systems aren't as inefficient when it comes to tape backup, they probably still could benefit from virtual tape's reliability and speed, he says.

Virtual tape evolves

The concept of virtual tape systems isn't new, as IBM introduced the idea for its S/390 mainframes in the mid-1990s. The company's IBM 3494 Virtual Tape Server was meant to take the place of numerous bulky 3494 Tape Libraries and save floor space, improve tape utilization, reduce tape mounts and improve performance by eliminating the physical movement of tape. StorageTek and Fujitsu Siemens subsequently introduced their appliances for mainframe environments.

"On the mainframe, the process of writing data sets to tape often left the tapes with a lot of empty space," says Dave Hill, senior analyst with Mesabi Group. "With virtual tape, multiple data sets are concatenated on disk and then written to tape," thus achieving better utilization.

The advent of inexpensive Serial Advanced Technology Attachment (ATA) disks has made virtual tape libraries an affordable alternative to tape backup, proponents say. While the ATA drives that most appliances use are not as inexpensive as tape, their reliability and speed of recovery make them competitive.

Virtual tape appliances fit in the network between file and media servers and the back-end storage-area networks (SAN) and tape libraries.

Andrew Ferguson, manager of enterprise operations for Brookhaven National Laboratories in Upton, N.Y., chose a virtual tape library appliance from Sepaton to back up a Windows network environment. Before using Sepaton's S2100-ES, the Brookhaven network consisted of multiple, separate back-up environments such as for Microsoft Exchange and for database servers.

"We wanted to get these islands of backup under one enterprise product," Ferguson says. "We also wanted to centralize our tape changers."

Sepaton's offering looks like a tape library but is a lot faster, says Ferguson, who backs up 17T bytes of data from a Dell/EMC SAN.

Virtual tape and tape libraries will supplement traditional tape technology over the next few years, according to Alex Gorbansky, an analyst at Taneja Group.

"Tape is going to continue to have a role as nearline and long-term archival media," he says. "As people will start to maintain more data online, virtual tape will start to eat into some of tape's capability as a nearline repository."

Brookhaven's Ferguson has adapted his tape backup for just that use.

"We now go to tape only if we need to for archiving or if for some reason we need to take a tape out of the environment and do a restore into another environment," he says.

Some virtual tape library packages such as ADIC's Pathlight VX, Fujitsu Siemens' CentricStor and Neartek's Virtual Storage Engine already include provisions for migrating data from the disk-based virtual tape system to tape. These offerings don't require IT to use back-up software to copy data from the virtual tape system to a physical tape library and then to tape without involving the media server. ■

Better than tape?

A sampling of virtual tape library offerings, the first versions of which were mainly for mainframes

Product	Year introduced	Product form	Platforms supported
ADIC's Pathlight VX	2003	Appliance includes Serial ATA disk	Unix/Windows NT
Alacritus' Securitus	2001	Appliance only	Unix/Windows NT
Diligent's Virtual Tape Facility Mainframe and Open	2002/ 2003	Appliance only	Mainframe and Unix/Windows NT
EMC's Clariion DL300 Disk Library	2004	Appliance includes Serial ATA disk	Unix/Windows NT
Fujitsu Siemens CentricStor	1999	Appliance includes Fibre Channel and Serial ATA disk	Mainframe and Unix/Windows NT
IBM's 3494 Virtual Tape Server	1993	Appliance includes disk storage	Mainframe
Neartek's Virtual Storage Engine VSE2	2002	Appliance only	Mainframe and Unix/Windows NT
Quantum's DX-Series Disk-based Backup System	2002	Appliance includes Serial ATA disk	Unix/Windows NT
Sepaton's S2100-ES Virtual Tape Library	2003	Appliance includes ATA disk	Unix/Windows NT
StorageTek's Virtual Storage Manager and VSM Open	1998/ 2003	Appliance includes StorageTek Shared Virtual Array and Fibre Channel	Mainframe and Unix/Windows NT

More online!

Follow the latest in the storage market with Senior Editor Deni Connor's storage research center.

DocFinder: 6438

How Does BMW Deliver Application Performance on the WAN?

BMW deploys FineGround. By installing the FineGround application delivery appliance in their data center, they deliver LAN-like performance to their remote operations, employees, and users around the globe. No remote boxes. No infrastructure upgrades. And no application rewrites.

If your organization has a global user base, FineGround has the solution for delivering your business-critical applications. Contact us today for a free proof of concept. We'll show you how your web business can perform.

www.fineground.com/BMW

1.866.WAN2LAN

FineGround™
How Web Business Performs

Physics project relying on giant computing grid

■ BY JAMES NICCOLAI

If the Large Hadron Collider at famed Geneva laboratory CERN is to yield miraculous discoveries in particle physics, it also might require a small miracle in grid computing.

Undaunted by a lack of suitable tools from commercial vendors, engineers at the lab are hard at work building a giant grid to store and process the vast amounts of data the collider is expected to produce when it begins operations in mid-2007. They announced last week that the computing network now encompasses more than 100 sites in 31 countries, making it what they believe is the world's largest international scientific grid.

Inside the collider, proton beams traveling in opposite directions will be accelerated to near the speed of light and steered into each other using powerful magnets. Scientists say they hope to analyze data from the collisions to uncover new elementary particles, solve riddles such as why elementary particles have mass, and get closer to understanding how the universe works.

The proton collisions will produce an estimated 15T bytes of data each year. The role of the grid is to link a vast network of computing and storage systems and provide the scientists with access to the data and processing power when they need it.

The grid sites involved are mostly universities and research labs as far afield as Japan and Canada, and two HP data centers. The sites are contributing computational power from more than 10,000 processors in total, and hundreds of millions of gigabytes in tape and disk storage.

Much of the data will be stored in Oracle databases. Most of the middleware will be homemade.

Niccolai is deputy news editor at IDG News Service.

Fault-tolerant

continued from page 21

Linux community and hopes to support standard distributions of Linux by year-end, Lane says. Stratus also supports VOS on its Intel-based servers.

The Boston Stock Exchange, which plans to deploy its Intel-based, fault-tolerant server in April, is not alone in looking at lower cost alternatives.

The Federal Aviation Administration (FAA) recently announced that it was migrating its message-switched network off of aged Philips DS714 mainframe computers and onto four of Stratus' Xeon-based ftServer 6400s.

The FAA's National Airspace Data Interchange Network handles data filed by every plane that enters or leaves American airspace. The network, which processes more than 1.5 million messages per day, is the data interchange between the U.S. and other nations to communicate flight plans for commercial and general aviation and weather and advisory notices to pilots.

Downtime is not an option. But while the FAA was looking for a reliable system, it also wanted something that would be economical and easy to manage. The mainframes the agency was using, originally manufactured in 1968 and upgraded with new processors in 1981, had been getting increasingly harder to maintain, support and write code for.

"We looked at a lot of products, including HP NonStop computers. But there are not many out in the market, and it really boiled down to Stratus offering a more cost-effective solution," says Andy Isaksen, computer scientist for the FAA in Atlanta.

The Stratus ftServer "offered us the opportunity to program in the Windows environment, which made a few people nervous, but Stratus has been in the Windows fault-tolerant market for a long time," Isaksen says.

Isaksen will install two Stratus ftServers in his production network — one in Atlanta and the other in Salt Lake City. Two other identical servers are part of a test bed for running applications.

"The two centers run in a load-shared mode and at any instance can take over for each other," Isaksen says. "If one server dies, the other one almost instantly takes over so there is no loss of service to the aviation community."

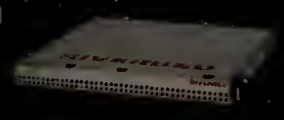
The servers will be deployed in April and go online by early next year, Isaksen says. ■

This is what we have in mind for your WAN.

Most applications and protocols were designed to run locally. Over a WAN, they grind to a halt. That's why Riverbed developed a solution built on radically new, patent-pending technology that actually delivers LAN-like performance across your WAN. Even for chatty applications that can break down across the most robust networks.

Riverbed's proven solution allows your enterprise to consolidate IT infrastructure at the data center, optimize your bandwidth usage, and still deliver applications and data over your WAN – at speeds that make remote data feel local.

We're so confident that Riverbed can improve your WAN application performance, we'll even let you try it for 30 days, risk-free. Call us at **1-87-RIVERBED** to get started right away, or visit **www.riverbed.com/NW** today.



RIVERBED

THE BRAINS TO BACK IT UP.

PATHLIGHT VX
Disk-Based Backup

Looking at disk-based backup but not sure how to make it happen? Get the smarter disk backup solution—Pathlight® VX 2.0 from ADIC, the leading provider of tape libraries for open-systems backup.*

Smarter disk-based backup. Pathlight VX 2.0 uses advanced policy-based data management to merge the capacity of disk and tape into a single, unified solution. Disk gives you twice the backup performance of conventional libraries—and even faster restore. Tape delivers scalability, value, secure retention, and flexible disaster recovery. You get the best of both technologies in a single solution that slips right into your existing backup system.

Clear investment protection. With Pathlight VX 2.0, you can boost your backup and restore whether you need a system for 3.8 TB or 3,000 TB—and pay a lot less for it. You can even use your own tape library as part of the system—tape storage can be supplied by one of ADIC's intelligent Scalar® libraries, or by your legacy StorageTek L-Series™ system.

Room to grow, smarts to save. Pathlight VX 2.0 delivers all the performance of disk and the fault tolerance of RAID, but it also scales to meet enterprise capacity demands and grows easily with your data—and it can cut your costs in half or more compared to conventional products.

*Market share from Gartner Dataquest, Tape Automation Systems Market Shares, 2003, F. Yale, April 2004.

Visit ***www.adic.com/pvx*** to get your free GlassHouse white paper
by W. Curtis Preston, *Evaluating Disk-Based Backup Solutions.*

adic

Intelligent Storage™

Application Services

■ CRM ■ MESSAGING/COLLABORATION ■ WEB SERVICES
■ ERP ■ E-COM ■ NETWORK AND SYSTEMS MANAGEMENT

Short Takes

■ **Maven Networks** now is offering its **intelligent Delivery Service** to customers that want to add on-demand video delivery to current networks and applications. Intelligent Delivery includes a range of pre-built components that are designed to help manage video caches and deliver video in the background. It also has application services for such things as digital rights management. Maven has offered Intelligent Delivery as a managed service for a few years with customers including AtomFilms and A&E Television Networks International. The cost the service will start around $50,000, depending on usage.

■ **Novell** last week acquired IT asset management company **Tally Systems** for an undisclosed sum in order to expand its ZENworks product line. Tally offers tools for discovery and inventory, license management and analysis of software usage and trends. Novell says it wants to use its technologies to improve its ZENworks system management offerings to give customers a greater ability to track corporate systems and information. Tally says it has products licensed on more than 10 million PCs and 15,000 Web sites. The Lebanon, N.H., company offers products with capabilities such as patch management, application self-healing and software deployment.

■ **EMC's Documentum unit** last week unveiled a retooled **content management platform,** plus a slew of new products to go with it. The platform features a unified architecture that combines traditional content creation, management, delivery and archival services with a unified repository and set of collaboration, federated search and retention management products. To simplify implementation and management, all the pieces share a common code base, security model, repository, object model and API, EMC says.

Call mining gets a boost

■ BY ANN BEDNARZ

Recording telephone conversations between customers and agents is commonplace in call centers. Usually it's done for quality or regulatory purposes with technology that automatically records, logs and stores the audio files.

What happens to those recorded assets often is considerably less high-tech. A manager might randomly select a few phone calls per month for each agent and listen to replays to evaluate agent performance. Or training staff might single out calls that resulted in a strong sale to use for educational purposes. But often companies simply ignore the bulk of recorded assets because it's too expensive and time-consuming to manually review thousands of customer phone calls.

These days, call-mining specialists such as CallMiner and Nexidia and larger speech technology vendors such as ScanSoft and Witness Systems are aiming to change that with technology that does for audio assets what business intelligence software does for structured data.

Call-mining technology combines speech recognition, speech analysis and data-mining capabilities to make it easy for companies to find specific information in audio archives and spot service gaps, sales opportunities and emerging customer trends.

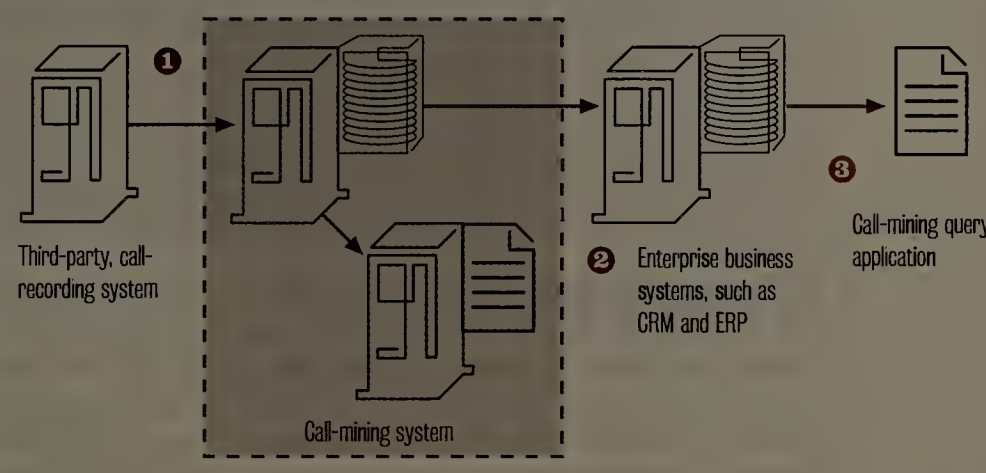
The software can run keyword-based searches to find instances when callers spoke certain product names or used phrases associated with dissatisfaction such as "speak to a manager." The software also correlates different attributes of calls to report trends — such as how often the mention of a competitor's product resulted in a service cancellation.

One prison uses technology from start-up CallMiner to ferret out code words for contraband. The CallMiner software stores reference data about word-usage trends and can highlight when words that are not frequently used in normal conversation suddenly increase in prisoners' phone conversations, says Jeff Gallino, CEO of CallMiner.

In the past, by the time officials figured out "lollipop" was a code word for a certain drug, for example, the prisoners already would have started using a new code word. CallMiner's speech analytics can detect within a couple of hours when an atypical word suddenly is used more frequently, Gallino says.

Audio assistance

A typical database-driven, call-mining platform converts recordings into text and lets users run queries against the stored conversation data.



1. A call-mining engine uses speech-recognition technology to convert telephone recordings into text, which then gets stored in a relational database.
2. Users can conduct ad hoc queries on mined data. In addition, packaged reporting options can include call scoring and classifying features, based on customer-defined criteria.
3. By linking a call-mining application to existing CRM or ERP systems, companies can correlate customer service issues with product and sales information.

Call-mining software also can search for phrases that agents didn't say — but maybe should have been by agents for legal reasons. For example, financial services transactions can require agents to cite regulatory disclosures to customers. Companies can search for instances when those disclosures were not made, but should have been, says Anna Convery, senior vice president of marketing and product management at Nexidia.

Continental Airlines is one early adopter that's rolling out call-mining software. The airline uses eQuality CallMiner — a call-mining platform that combines technology from CallMiner and Witness Systems — to perform automated call classification processes at its 900-agent reservation center in Tampa, Fla.

Continental classifies incoming calls into 50 different categories, depending on

See Mining, page 32

Customization comes to low-end CRM software

■ BY STACY COWLEY

The knock against low-end CRM software traditionally has been that it takes a one-size-fits-most approach that does not work for businesses with complex processes. If users need customization, they are steered toward the wares of enterprise vendors — with their correspondingly high enterprise-class price tags. But as vendors in the crowded market advance their technology and look for competitive advantages, sophisticated customization features are creeping into less expensive applications.

NetSuite last week took the wraps off a set of capabilities it dubbed NetFlex, aimed at making NetSuite's ERP CRM/e-commerce applications bundle a flexible, standards-compliant platform that can adapt to custom business needs. The move parallels rival Salesforce.com's preview of a package due in June, called Multiforce, which will let users add new features and applications to run within their Salesforce.com system.

At the heart of both company's updates are tools designed to let users customize their systems without digging into pro-

See NetSuite, page 32

Intelligent Infrastructure, Intelligent Business

Overlaying the Internet with an intelligent infrastructure unleashes the next generation of business potential

As amazing a business tool as the Internet has become, the fact remains that organizations have just scratched the surface of its far greater potential. The ability of Voice over IP (VoIP) to radically reduce fundamental communications costs is one early indication of the Internet's transformational capabilities. The unique insight into Internet security patterns and trends can allow a managed security services provider to give businesses the extra measure of security protection demanded today. Radio frequency identification (RFID) projects are literally redefining the way manufacturers and their partners interact. From these examples and others, it is clear the emergence of intelligent infrastructure services is bringing the potential of the Internet to full flower.

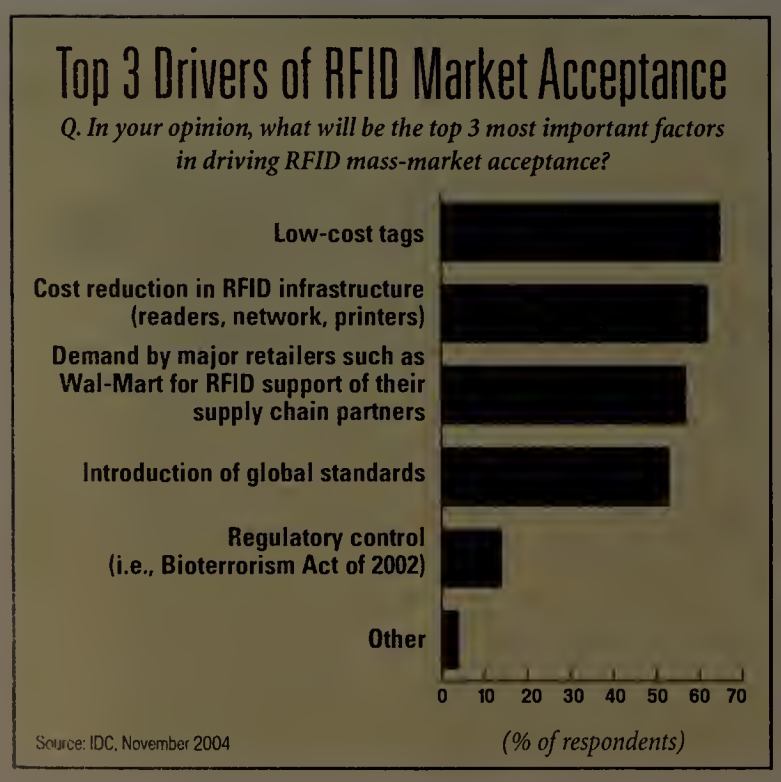
It would be more than three decades before the short-haul railroads that sprung up everywhere starting in the 1830s would finally be interconnected and transformed into a national rail system. This took such a long time simply because railroad operators had to use sluggish, unreliable overland mail services to coordinate this vast effort.

But once telegraph lines were installed right alongside the rail beds, two-way communication became almost instantaneous. Rail development soared as a vast national network took shape. And it all happened because the original system was overlaid with an *intelligent infrastructure: the telegraph network.*

Thus, a network faced with a critical level of usage and a growing complexity threatening its usefulness was instead transformed into a veritable engine of progress and growth. The rest, as they say, is history.

The same can be said today about the Internet. This network of networks holds almost limitless potential to link businesses to partners, suppliers, and customers in dynamic, interactive ways. The vision of a supercharged Internet will reach its full potential only if these links and connections can be made secure, reliable, and adaptable. In other words, like the early railroads of 175 years ago, the Internet needs an overlay of intelligent infrastructure. The Domain Name System (DNS) was the critical intelligent infrastructure that linked requests for user-friendly domain names to more complex IP addresses, which helped make the Internet accessible to the masses. Similarly, intelligent infrastructure will play a critical role in unlocking the tremendous business potential of the Internet as it grows.

Think of it this way: Intelligent infrastructure for the Internet will provide several, if not all, of the following key network enhancements—scalability, security, interoperability, availability, adaptability, and visibility—to literally change business processes and their economics. Already, intelligent infrastructure is enabling some of the most exciting business applications, such as VoIP, highly touted RFID-enabled supply chains, and mobile digital content delivery systems. And that's just for starters.



The drivers

Like the telegraph of a bygone era, intelligent infrastructure and intelligent infrastructure services are not technologies in search of a market or application. Quite to the contrary, the development of intelligent infrastructure services is intimately linked to today's major business and network drivers. These drivers include:

- **The growing use of the Internet for mission-critical applications.** During the year-end holiday shopping period last year, shoppers placed some $9 billion of orders online. That number should double in three years. But growth will be stopped dead in its tracks and even recede rapidly if consumer confidence in secure online transactions doesn't continue to grow in tandem.
- **The rapidly rising tide of regulatory compliance.** The business lexicon today is spiked with an alphabet soup of acronyms referring to new compliance regulations related to business data. From SOX to HIPPA to CALEA and so on, these regulations are placing heretofore unheard-of demands upon IT managers to maintain a scalable security framework to comply with internal and external audit requirements.
- **The fight against phishing and identity theft.** These two culprits, left unchecked, would be a big glass of icy cold water thrown in the face of Internet commerce, and the ramifications would be disastrous for so many kinds of organizations that have invested so heavily in e-commerce infrastructures.
- **The interoperability mandate.** Everyone knows that business-critical communication is trending outside the four walls of the organization or, in network terms, far beyond the firewall. The most important network and data links are among a business and its partners, customers, and suppliers. If the underlying network infrastructure doesn't have the intelligence to recognize and accommodate the disparate systems it inevitably encounters, growth of these vital communications links will surely be stunted.
- **The business continuity mandate.** Several years ago an industry pundit declared, "The network is the computer." The contemporary version of that truism is: "The network is the *business*." Just ask executives at an airline or hotel, or a modern manufacturing operation. If workers and

smart machines can't access and swap information, work for all practical purposes grinds to an ugly halt. Real costs accrue. Jobs and careers are jeopardized. The network has to be solid and stable, without compromise.

VeriSign answering the call to action

While the items above are noted as "drivers," IT managers usually refer to them as "formidable challenges," among other things. For IT managers, who have been working on very tight budgets over the last several years and are being pushed to support core business requirements and applications, the mere thought of meeting these challenges is daunting.

This is where VeriSign enters the fray. With its focus on providing and shaping the Internet's intelligent infrastructure, VeriSign is singularly dedicated to enabling businesses to find, connect, secure, and transact across today's complex Internet, telecommunications, and converged networks.

Perhaps most widely known for its Domain Name Registry Services, VeriSign in fact operates an intelligent infrastructure that processes an astonishing *14 billion* Web and email lookups each day. In North America, the greatest of all commercial marketplaces, VeriSign handles more than 37% of all e-commerce transactions, securely processing some $100 million in daily online sales.

By leveraging its rich and deeply experienced Internet legacy along with key technology acquisitions made in recent years, particularly in the digital content management area, VeriSign is positioned as the leader in providing intelligent infrastructure services at just the right time in business history.

Intelligent infrastructure in action

In many ways, intelligent infrastructure is synonymous with the most exciting aspects of network convergence and the blossoming of next-generation networks. VeriSign's expertise is already delivering results to IT professionals. In the red-hot area of Managed Security Services (MSS), VeriSign has leveraged its unique experience and insight into Internet security patterns and trends to provide unparalleled intelligent MSS. These services hit many IT security sweet spots, such as the growing problem of phishing or identity theft, as well as endpoint protection and managed vulnerability protection services.

"As enterprises face external forces that impact their business, such as hacker attacks, and cost, compliance, and complexity issues, they are looking to Managed Security Services Providers to help them with their network security. However, point solutions and MSSPs without unique differentiators do no good. With cyber attacks increasing in size and sophistication, they need unique insight into trends within their networks, across networks, and the Internet to make sure appropriate security protections are taken."

—Judy Lin, Executive Vice President and General Manager, VeriSign Security Services

When it comes to RFID-enabled supply chains, where electronic "tags" are poised to replace the current barcode system, VeriSign is making it possible for manufacturers and their partners to get more fine-grained, real-time inventory intelligence. Forrester Research maintains that new intercompany RFID projects will require advanced technologies to manage the sheer volume and complexity of RFID data. Forrester says partnerships between VeriSign and leading data synchronization vendors will help companies leverage and exploit RFID while at the same time preserving existing technology investments. Developments in RFID are providing scalable IP data sharing and trust services, enabling demand-driven supply chains, and increasing visibility.

VoIP carries the promise of sending a lot of today's communications costs through the floor. But for service providers to deliver on this promise to eager enterprise customers, they must first undertake a lot of basic blocking and tackling, such as providing secure connections to allow VoIP to pass through despite the large number of ports to be opened within a corporate firewall. VeriSign intelligent infrastructure services will provide all this and more to allow carriers to deliver the full benefits of VoIP while addressing their own needs to bridge Internet and telecommunications infrastructure.

VeriSign has also been active in the nascent digital content services area. A new VeriSign service offering allows mobile network operators to respond on a global scale to new service demands, from both businesses and consumers, for multimedia and interactive digital content delivered over mobile devices. These include intelligent messaging services to help businesses mobilize communication, collaboration, and workflow applications on just about any digital mobile device.

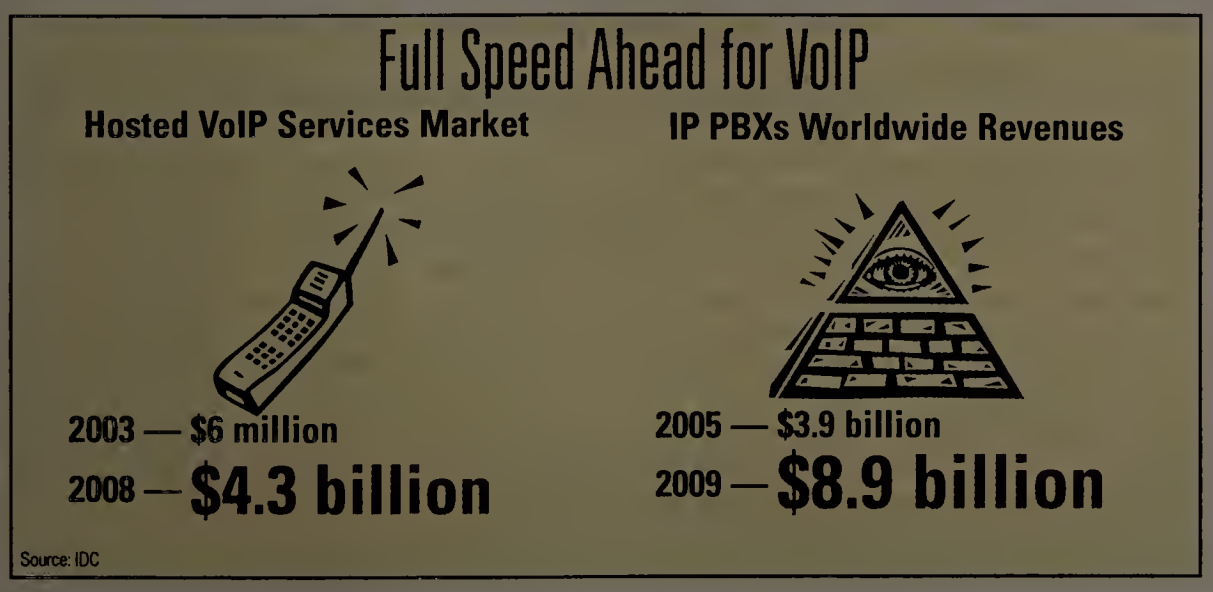
VeriSign®

A good example of intelligent infrastructure in operation is as follows: A sales executive is roaming on her cell phone (1), which switches over to an IP-based network (2), to make a transaction (3) in which content is secured (4) and delivered (5) back through that same connection. In this case, VeriSign has provided her with five different intelligent infrastructure services—transparent to her and the vital function she just fulfilled.

A matter of focus

This is just one example of how VeriSign has exploited its rich heritage of supplying Internet services to meet some of the most pressing challenges IT managers face as they struggle to meet today's hot IT issues of cost, complexity, and compliance. VeriSign is offering that overlay of intelligent infrastructure services essential to providing seamless, transparent interoperability among various network functions, clearing away obstacles to completing large IT projects that drive competitiveness.

Ultimately this vision and experience can pay significant dividends to enterprise IT managers who understand the potential of an Internet-based network overlaid by intelligent infrastructure services.



'NET INSIDER
Scott Bradner

Refusal, ignorance, arrogance or PR?

In mid-March, French news service Agence France Presse sued Google in a U.S. District Court for copyright violations. The news service demanded that Google stop including its material on the Google News site and asked for $17.5 million in compensatory damages. You will pardon me if I express some doubts about the actual motivation for this lawsuit.

I've written in the past about Google News (www.nwfusion.com, DocFinder: 6434). I consider it one of the most useful sites on the Internet. I use it to fill out the news snippets that I get from most other news sources. That said, I get frustrated at Google News links to subscription-only sites because I can't access some of the stories that look interesting. I've always assumed that such sites welcome Google's pointers because they get free advertising for themselves and thus might get some additional customers.

In that context, this lawsuit makes me wonder what's up with AFP. Google News doesn't show full articles, so I find it hard to understand what damage could mount up to more than $17 million — maybe AFP has a very high opinion of its ability to come up with inventive headlines and feels that other news organizations will rip them off if the headlines, which Google News does show, are visible. Or maybe the reason that AFP doesn't want Google News to point to its material is that AFP fears getting more subscribers will mean it would have to hire more people to deal with them.

Even if I don't understand why a company in the business of selling its services does not want more people to know about those services. It doesn't look like it would be all that hard for AFP to ensure that Google skips over its sites. Google has an easy-to-find Web page that says quite clearly how to keep a site from being scanned (www.google.com/remove.html). Basically, all you do if you want Google to skip all or part of your site is put one or more files named "robots.txt" in your Web site. For example, your whole site will be skipped if you have such a file at the root of your Web server containing these two lines:

User-agent: *
Disallow: /

Robots.txt files can get quite fancy (see DocFinder: 6435).

I suppose it's possible that the Google News Web crawlers don't pay attention to the robots.txt files that Google says it respects for its other Web crawling, but that doesn't seem likely. It is likelier that AFP somehow didn't know how easy it would be to do 2 minutes worth of work itself, on its own Web site, to ensure that its material would not be included. A tactic that would have taken far less effort than, as the news service claims to have done, pestering Google to try to get it to stop scanning. It also would have taken far less effort than filing a lawsuit. Well, maybe it's not all that likely that no one at AFP knew about robots.txt files — maybe there is some other reason it didn't take the easy path. The two that spring to mind are arrogance ("stop," said King Canute to the tide, "splash," said the tide to King Canute) or a desire for publicity.

Disclaimer: Of course you never see either arrogance or a desire for publicity in relationship to Harvard, so the above observation is mine alone.

Bradner is a consultant with Harvard University's University Information Systems. He can be reached at sob@sobco.com.

Mining

continued from page 29

whether a customer called to book a flight, confirm flight information, change a seat assignment or redeem reward miles. With eQuality CallMiner, Continental automates the process of compiling its "call mix" survey.

In the past, Continental completed monthly surveys, but now it can review the data daily, said Andre Harris, director of reservations training and quality for Continental Airlines, in a statement. The software provides more context and intelligence than manual methods, and management can review a much larger sampling of interactions, Harris said.

Mining momentum

There are two general approaches to call mining: speech-to-text and phonetic.

CallMiner's software is speech-to-text. It uses speech recognition to convert calls into searchable text, and uses speech-analysis techniques to generate call statistics about what was said and the conversation context. The data is stored in searchable databases for mining and gathering business intelligence.

Nexidia's software uses phonetics. The software breaks down audio into phonemes, which are speech sounds or utterances that represent one distinctive sound. For example, when a user runs a query for a word or phrase, the software identifies the relevant phonemes, then indexes and stores the results in a database for review.

Phonetic-based call mining is faster and handles searches for multilingual audio utterances more readily, Schoeller says. Speech-to-text processing tends to consume more CPU resources, he adds.

Speech-to-text advocates acknowledge that initial call processing can take longer, but say subsequent searches are more efficient because all the audio content already was converted into database form.

Typical early adopters, such as financial services companies, airlines, telephone and cable companies, and government agencies, have driven increased interest in call mining over the last few years, analysts say.

"The problem of not having enough hours in the day for supervisors to listen to calls to provide more training and feedback crosses many of these verticals," says Art Schoeller, a senior analyst at The Yankee Group.

Government agencies, in particular, are turning to call mining and speech analytics to help pore through huge amounts of audio secured for homeland security initiatives, says Daniel Hong, voice business analyst at Datamonitor. "If they use call mining, they're able to do that quite a lot faster, at a fraction of the cost, and on an on-going basis," he says.

Performance improvement is one reason for recent interest, according to Schoeller. In the past, processing audio files required a huge CPU commitment.

"At one time, it took a pretty hefty server one hour to process one hour of audio. You take a 100-agent call center, one-and-a-half shifts per day, you get 1,200 hours of audio to process," Schoeller says.

Today, some vendors say they can process 40 hours of audio for each hour of CPU time, Schoeller says. "We have also seen continued, gradual refinements in the algorithms themselves to improve accuracy and speed," he says.

Prices have become more affordable. Nexidia says it estimates a typical installation would cost between $100,000 and $300,000 — companies tend to grow their deployments as they get comfortable using speech analytics, Nexidia says. CallMiner says it estimates a 200-seat call center would spend about $450,000 for its call conversion engine and analytic suite.

Looking ahead, applications for searching audio and video will emerge outside the call center, Schoeller says. For example, a company might have in-house media libraries with training videos or presentations that could be indexed.

But it won't happen overnight. While expectations are higher, the reality of audio mining is that it's still an emerging science, and adoption remains in the early stages. ■

NetSuite

continued from page 29

gramming code. Salesforce.com's point-and-click tool is called Customforce; NetSuite's is AppBuilder.

NetSuite customer Barry Friedman raves about the customization he's done on NetSuite's system. Friedman is the CEO of BizActions, an e-mail newsletter technology company. While the company is headquartered in Potomac, Md., its staff is scattered throughout the country, thanks in large part to BizActions' ability to run operations through NetSuite's software.

Friedman has used AppBuilder to create a number of specialized applications within NetSuite such as programs for tracking renewals and collections, and a program that manages his company's telesales process via scripts.

"In my more than 30 years in accounting and technology, I've never seen software like this," Friedman says. "I literally manage the entire company from my dashboard."

NetSuite and Salesforce.com offer their customization functions at no extra cost to customers of their full-featured editions. Both are hosted service providers, which maintain and manage their applications on a subscription basis.

Meanwhile, Microsoft is preparing a major update of its CRM application, scheduled for release in late 2005, which significantly will increase its adaptability. Microsoft first released its closely watched Microsoft CRM software at the end of 2002 and has performed one major update since then. But the current software has limited functionality, some frustrating glitches relating to software synchronization, and limited integration with Outlook e-mail and information management client. The next version will be a significant leap forward, according to Microsoft executives and those who have had early access to the new product.

Key to the update will be the ability to add entities, records that carry throughout the system and can be customized, says Sheryl Kingstone, an analyst at The Yankee Group. She says she expects Microsoft's forthcoming integration, data management, and workflow improvements to put Microsoft CRM on par with its rivals.

One mystery still surrounding Microsoft's software is its name. Initially referred to as Microsoft CRM 2.0, the overhaul briefly became Microsoft CRM 2005, before reverting back to unnamed limbo, according to Microsoft CRM General Manager Brad Wilson. Microsoft says it promises that more information about the update, including its name and a detailed feature set, will be out in the third quarter of this year.

Cowley is a correspondent with the IDG News Service.

IBM

WebSphere.

Key

1. **Deductible viewed quickly.**
2. **Claim info filed accurately.**
3. **Vendor receives complete data.**
4. **Quotes researched easily.**
5. **Great service boosts policy sales.**

MIDDLEWARE IS IBM SOFTWARE. Powerful WebSphere software. For an integrated IT environment that makes your business more flexible. WebSphere delivers a secure, scalable platform. Enabling a service-oriented architeoture. So your business can respond faster. More efficiently. To partners, vendors and customers. With no ripping. No replacing. No headaches. No kidding.

Middleware for the on demand world. Learn more at **ibm.com**/middleware/flexible ON DEMAND BUSINESS™

IBM Workplace.

Key

1. **IMs stockroom for '01 merlot.**
2. **Conferencing with design partners.**
3. **Orders from vendor, wirelessly.**
4. **Driver receives last-minute order.**
5. **Delivers orders quickly, accurately.**

MIDDLEWARE IS IBM SOFTWARE. IBM Workplace transforms productivity. Collaborate better with colleagues, partners and suppliers – the whole team. IBM Workplace offers fast access to critical information based on your role. With all of the collaborative tools you need to work efficiently in one environment, you can make better, more informed decisions. Faster. It's simply a better way to work.

Middleware for the on demand world. Learn more at **ibm.com**/middleware/workplace ON DEMAND BUSINESS™


4
1
5
IBM

Service Providers

■ THE INTERNET ■ INTEREXCHANGES AND LOCAL CARRIERS
■ REGULATORY AFFAIRS ■ CARRIER INFRASTRUCTURE

Uniting carriers against 'Net attacks

■ BY DENISE PAPPALARDO

Arbor Networks says it is attempting to make it easier for service providers to share information about Internet threats through a new program called the Fingerprint Sharing Initiative.

The program, being introduced this week, uses Arbor's PeakFlow SP platform, which is used by service providers to sniff out distributed denial-of-service (DDoS) attacks, worms and other security threats on their own networks.

The latest version of PeakFlow SP includes a Fingerprint Sharing option that lets carriers share attack fingerprints with any PeakFlow SP customer that is using the option while an attack is underway.

"There's nothing like this that effectively lets far-flung network operators have direct, real-time information sharing," says Jim Slaby, a senior analyst at The Yankee Group.

Mazu Networks, Lancope and Q1 Labs offer Arbor-like products for enterprise networks, but Arbor has cornered the carrier market, he says.

Officials at MCI, one of the service providers participating in the Fingerprint Sharing Initiative, say the program is one instrument in a toolbox used to thwart attacks. While sharing information about DDoS and worm attacks is not new at MCI or among the ISP community (www.nwfusion.com, DocFinder: 6437), Arbor's initiative is an advance because it provides for real-time information exchange, says Chris Morrow, senior network consulting engineer at MCI.

Also, current methods did not provide the same level of traffic trending, Morrow says.

Arbor creates a registration database of participating service providers. Once a company registers, it can communicate directly with PeakFlow SP devices on peers' networks.

PeakFlow SP products watch and analyze traffic patterns to determine the type of packets that are causing problems, as well as the source network.

While the Fingerprint Sharing Initiative requires that ISPs have a PeakFlow SP device, Arbor says it is in the process of standardizing the procedure so that even carriers that aren't its customers can take advantage of the technology.

Arbor plans to submit a draft proposal through the IETF's Extended Incident Handling Working Group, with hopes for its initiative to become a standard in six to 12 months. ■

Sharing DoS attack info

These organizations are publicly acknowledging their involvement in Arbor's Fingerprint Sharing Initiative:

- Asia Netcom
- BT
- Deutsche Telekom
- EarthLink
- ITC DeltaCom
- Merit Network
- NTT Japan
- Rackspace Managed Hosting
- The Planet
- University of Pennsylvania
- Utah Education Network
- Verizon Dominicana
- WilTel Communications
- XO Communications
- MCI

Short Takes

■ **BellSouth** this week announced a **Centrex service** it says integrates wireline and wireless calling. BellSouth Centrex Simultaneous Ring concurrently delivers incoming calls to up to five phones at a customer's location. One of these numbers can be a cell phone. Simultaneous Ring costs $5 per month per station. There is a one-time install charge of $8 per station. The service is available to new or current Centrex users and is one of many enhancements BellSouth has made of late to its network-based service.

■ **MCI** last week announced a major expansion in the number of **wireless hot spots** available to its large business customers. The carrier has launched 1,300 Wi-Fi hot spots in Europe and the Asia/Pacific region, and will launch 3,400 hot spots in the U.S. in May, the company said. MCI's wireless service corporate customers had access to about 6,200 hot spots worldwide before the expansions. The effort will bring hot spots to cafes, bookstores and business service centers. MCI offers an unlimited Wi-Fi plan for $40 per month as an add-on to dial-up service. A time-based plan charges $8 an hour for the first hour, with a maximum of $15 per day.

Shaping an SLA

EYE ON THE CARRIERS
Johna Till Johnson

Recently I stressed the importance of contracts that define effective service-level agreements and include escalation procedures for ensuring effective enforcement. Many companies gloss over SLAs, or tack them on at the very end of the negotiation cycle. That's a big mistake. SLAs should be as integral to the negotiation process as price, and telecom managers should craft them carefully.

I touched on the critical components that should go into an SLA. Now let's talk about them in depth:

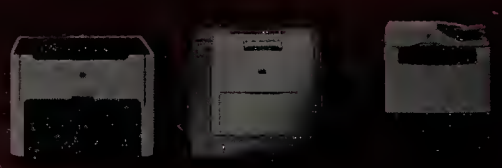
- **Performance.** SLAs should specify end-to-end latency, jitter and packet loss. If the provider offers multiple QoS classes, the SLAs should be defined for each class. And SLAs should include average and maximum levels both for individual circuits and the network as a whole. Additionally, penalties should accrue both for chronic and acute failures to comply. In other words, there should be penalties for consistently failing to meet SLAs, even if the performance is only slightly worse than contracted for (regularly delivering 60 ms end-to-end delay instead of 50 ms, for example), as well as for extreme failures to comply such as a single instance of the latency spiking up to 200 ms. Naturally, this means that companies should plan to monitor and record performance on an ongoing basis — in addition to the monitoring statistics the service providers provide.
- **Provisioning.** SLAs should specify average and maximum provisioning times for all types of services, including new-circuit installations, turning up VPN services, and activating calling cards and other voice services. Moreover, the excuse that "it's all the local exchange carrier's fault" is now increasingly out-of-date: If AT&T, for example, is now part of SBC, then the combined company is responsible for services from soup to nuts (at least within SBC's region of operations). No more excuses.
- **Response and repair times.** Service providers should specify exactly how long it will take them to respond to trouble-tickets and requests, and how long it will take them to restore service. And once again, telecom managers shouldn't be content with averages or mean times — they should ask telcos to define maximum response and repair times. Because extremely rapid response-and-repair times may cost more, it's reasonable for telco managers to define tiered response-and-repair times for sites with different availability requirements. This also can be helpful with internal charge-back: Telco managers can charge more for sites that need higher uptime.
- **Escalation procedures.** Providing — and adhering to — detailed escalation procedures is the mark of a superior service provider. Telco managers should know exactly what will happen in the event that the above SLAs are breached, when the issue will be escalated, and to whom. Carriers should proactively notify customers when an issue has been escalated, and provide regular updates, even when the problem has yet to be resolved.

Getting all this into the contract isn't always easy, and often requires several rounds of negotiations. Telecom managers should be prepared to invest the time and energy upfront. They'll be glad they did.

Johnson is president and chief research officer at Nemertes Research, an independent technology research firm. She can be reached at johna@nemertes.com.

Your presentation is due now.
Your toner is due in two days.

(Isn't it time for a better printer?)



You can't afford not to buy an HP printer.

hp invent

HP LaserJet 1320 Printer

- Print speed: up to 22 ppm black
- Resolution: 1200 x 1200 dpi
- RAM: 16MB std., 144MB max.
- Paper handling: 250-sheet input capacity standard
- Duty cycle: 10,000 pages per month
- 1-year limited warranty

$399.99 PRINTER CDW 680841

$100 MAIL-IN REBATE AVAILABLE

HP Color LaserJet 3700n Printer

- Print speed: up to 16 ppm black and color
- Resolution: HP ImageREt 2400
- RAM: 128MB std., 448MB max.
- Paper handling: 350-sheet input capacity standard
- Duty cycle: 55,000 pages per month
- 1-year, next-business day, onsite warranty

$1599.99 PRINTER CDW 573050

-400 INSTANT SAVINGS[2]

$1199.99

HP LaserJet 4345x mfp

- Print and copy speed: up to 45 ppm
- Resolution: up to 1200 x 1200 with HP FastRes
- RAM: 256MB std., 512MB max.
- Paper handling: 1100-sheet input capacity standard
- Scanner and digital sender resolution: 600 x 600 dpi
- Automatic duplexing
- Analog fax

$3449.99 PRINTER CDW 699859

-249 INSTANT SAVINGS

$3200.99

With some printers, you can only order cartridges from the manufacturer. With an HP printer, you can get cartridges from CDW or anywhere that sells them. And that's just one of the ways HP saves you now and for years to come. Get the printer and supplies you need. Get an HP printer from CDW.

CDW

The Right Technology. Right Away.™

CDW.com • 800.399.4CDW

In Canada, call 800.387.2173 • CDW.ca

[illegible] mail-in manufacturer rebate; offer ends 6/25/05. [2]Price reflects $400 instant savings; call your CDW account manager for details; offer ends 6/30/05. Price reflects $249 [illegible] manager for details; offer ends 4/30/05. Offer subject to CDW's standard terms and conditions of sale, available at CDW.com.

Technology Update

■ AN INSIDE LOOK AT TECHNOLOGIES AND STANDARDS

802.11i secures wireless LANs

■ BY PAUL FUNK

The IEEE's initial attempt at wireless LAN security was Wired Equivalent Privacy. This turned out to be a quite unfortunate moniker, as WEP was quickly shown to provide very little of the privacy it advertised.

802.11i improves on WEP by using completely new encryption algorithms and key-derivation techniques. This wireless security standard, finalized in 2004, makes it possible to safeguard over-the-air communications at Layer 2.

A key called the Pairwise Master Key (PMK) is established between the wireless station and the access point. This key is typically generated using 802.1X, which is authentication of the user to a RADIUS or other authentication server using Extensible Authentication Protocol. Both the station and RADIUS server derive identical keys, and the RADIUS server returns that key to the access point.

Next, the station and access point exchange a sequence of four messages, called the "four-way handshake." In this exchange, the PMK and freshly generated random values from both station and access point are used to derive a new key, called the Pairwise Transient Key. This key is subdivided into several keys: one to sign four-way handshake messages; one to secure data packets transmitted between station and access point; and one to encrypt a "group key" to the station during the four-way handshake. The group key lets the access point broadcast one multicast packet to all stations, rather than send a separately encrypted packet to each station.

During the four-way handshake, the station and access point negotiate the type of encryption to be used for the data connection. Two encryption ciphers are negotiated: The pairwise cipher is used for unicast data between station and access point, and the group cipher is used for broadcast/multicast traffic from the access point to multiple stations.

While any encryption cipher may be negotiated, the cipher of choice for 802.11i is Advanced Encryption Standard (AES), with a 128-bit key, in Counter with CBC-MAC (CCM) mode. AES is the U.S. federal government standard for encryption. CCM is a very well designed mode of operation and recently has been approved as Federal Information Processing Standard-compliant.

In an 802.11i-only environment, AES normally will be used both as the pairwise and group cipher. In a mixed environment, access points typically will use a lowest-common-denominator cipher as the group cipher, such as WEP or Temporal Key Integrity Protocol, to let both 802.11i and pre-802.11i stations decrypt multicast traffic.

802.11i also speeds roaming from one access point to the next. Previously, it was necessary for the station to perform a complete 802.1X authentication each time it associated with a new access point. With 802.11i, when the station returns to an access point it already authenticated with, it can reuse the PMK established with that access point to omit 802.1X authentication and perform only the four-way handshake. This greatly speeds up transitions between access points. Additionally, the station may pre-authenticate to a new access point it intends to roam to, while still associated with the current access point; this lets the station only perform a four-way handshake once it roams.

Another fast-roaming technique made possible by 802.11i is informally called Opportunistic Key Caching (also Proactive Key Caching). If multiple access points can share PMKs among themselves, it is possible for the station to roam to a new access point it hasn't visited before and re-use a PMK established with the previous access point; this lets the station quickly roam to access points it never authenticated to, without even having to perform pre-authentication.

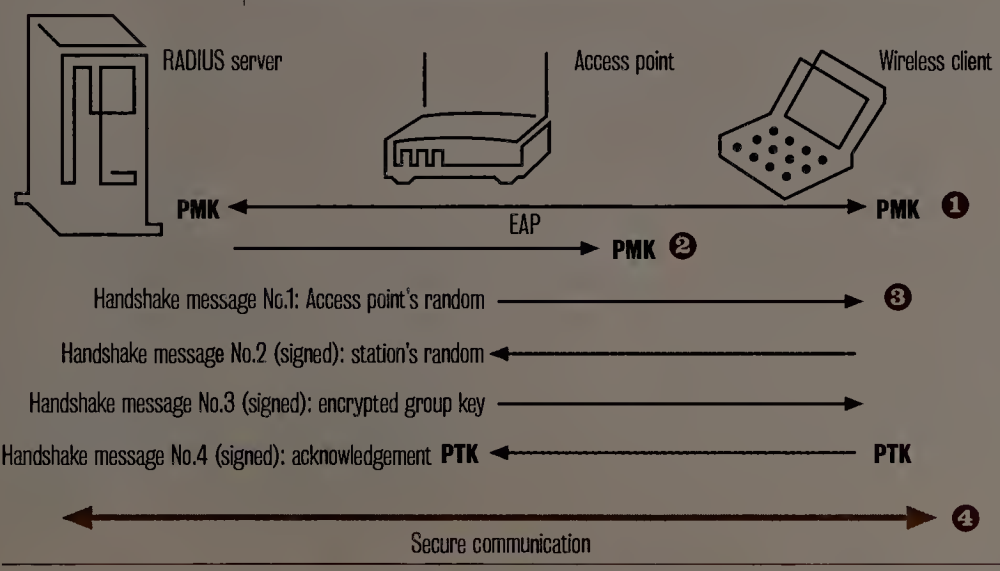
To deploy 802.11i, you'll need the following three hardware/software elements, each of which must support that standard:

- The "supplicant," a piece of software that sits on the hardware device you want to authenticate, performs high-level functions such as 802.1X and the four-way handshake.
- The wireless card/driver, which performs data encryption and communicates over the air with the access point.
- The access point, which provides the gateway to the network.

Funk is president of Funk Software. He can be reached at paul@funk.com.

■ HOW IT WORKS 802.11i

802.11i shores up wireless security by using new encryption algorithms and key derivation techniques.



❶ Client and RADIUS server perform Extensible Authentication Protocol (EAP) authentication via 802.1X to establish a shared key called a Pairwise Master Key (PMK).
❷ RADIUS server sends PMK to access point.
❸ Client and access point perform 802.11i four-way handshake to establish session key called Pairwise Transient Key (PTK).
❹ Data traffic now may pass between client and access point secured by Advanced Encryption Standard with PTK providing the encryption key.

Ask Dr. Internet

by Steve Blass

We have a Java application we would like to distribute as an executable for PC users. What tools for Eclipse developments can help us build a native executable version of our Java app?

GCJBuilder Eclipse plug-in integrates the GNU Compiler for Java (GCJ) into the Eclipse build process. GCJ compiles Java into directly executable programs. You will need GCJ, along with a copy of GNU Make, to use GCJBuilder with Eclipse. Links to GCJ and Minimal System (MSYS), which includes GNU Make, are available in the download section of the GCJBuilder Web site.

After installing GCJ and MSYS, adjust your system PATH so Eclipse can find the files "gcj" and "make." Unzip the GCJBuilder plug-in into your Eclipse plug-ins directory and start Eclipse. Follow the setup instructions on the GCJBuilder Web site to add GCLIB to your Eclipse Classpath Variables. Create a new Java project, open the Project Properties dialog, click on the checkbox labeled "Add GCJ Support," enter the name of your program's main class in the text box and click OK to close the dialog. Eclipse now will use GCJ to compile your Java source code and create the executable program in your project's "binout" directory.

Blass is a network architect at Change@Work in Houston. He can be reached at drinternet@changeatwork.com.

GEARHEAD INSIDE THE NETWORK MACHINE

Mark Gibbs

RocketVault: The final chapter

Our last two weeks of romping through the undergrowth of technology surrounding the Intradyn RocketVault touched on the device's SyncDR feature (See "Back that thang up!" www.nwfusion.com, DocFinder: 6448, and "Back that thang up — some more!" DocFinder: 6449). SyncDR allows near real-time, block-level synchronization of an SMB/CIFS share with a remote storage system that runs Secure Shell and rsync.

As we discussed, this remote system is preferably a Unix system, but Windows running Cygwin has been used (the limitation under Windows/Cygwin being a maximum file size of about 2G bytes).

When configured, the RocketVault SyncDR service contacts the remote storage device and makes a connection to the remote SSH service. After exchanging encryption keys and establishing a session, the RocketVault invokes rsync (which doesn't have to be running as a daemon). After that, any change made on the source share will be copied to the remote storage system.

A minor gotcha is that if the RocketVault cannot contact the SyncDR remote location -- for example, if a firewall is blocking the SSH port (Port 22) — the RocketVault will hang waiting for a reply. It would be nice if the RocketVault interface could test the remote location by pinging it and recover gracefully on failure.

The only snags with backing up remotely are that all client machines to be backed up need to be powered on and any files that are held open by applications or the operating system cannot be backed up (this includes operating system files, the Windows registry, Active Directory subsystem, application files and data files).

The former can be solved easily with a strip of duct tape over the big red switch while the latter is a little more problematic. A solution to this problem is Intradyn's BackAgain software that runs on the machine that is the source of the back-up data. BackAgain, available in both Windows server and workstation versions, can save backups on a RocketVault, a remote disk drive, or any standard tape drive.

When BackAgain encounters a file opened in exclusive mode it makes several attempts to back up the file before giving up (as opposed the RocketVault's single attempt). To ensure that files permanently opened in exclusive mode (which is the case with many operating system files) are backed up, Intradyn recommends Open File Manager (OFM) from St. Bernard Software.

OFM operates by tracking file transactions and cache changes that begin when a back up is started, providing the back-up application — in this case BackAgain — with a snapshot of all file data at the time the backup started. OFM allows live backups of any application. For a full explanation of OFM's operation see www.nwfusion.com, DocFinder: 6439.

We mentioned last week that the RocketVault has a few rough edges. Certainly it should be easier to set up the device and the documentation could do with an overhaul, but Intradyn pointed out that this product is usually set up by a dealer so the majority of users never will have to wrestle with these issues.

What users will have to deal with are the e-mail reports that the RocketVault generates. The reports are gobbledygook — unremittingly techie and full of extraneous detail that make them look more like debug traces designed by a committee of engineers who obviously had never met a live end user. It's not that you can't understand the reports, it's simply that the reports are overly hard to understand. Intradyn says this is on the list of improvements it is working on.

Despite our criticisms we really like the RocketVault. It works well, is reliable and delivers an excellent bang for the buck. The RocketVault line starts at about $1,500 with a 120G-byte drive (with compression this equates to roughly 250G bytes).

Speak your mind at gearhead@gibbs.com.

More online!

Follow along with Mark Gibbs' thoughts on an almost-daily basis in his Gearblog.

DocFinder: 6440

CoolTools

Quick takes on high-tech toys

By Keith Shaw

Travel highs and lows

I'm in Week 3 of an intense travel schedule that included a trip to New Orleans for the CTIA Wireless Show and two weeks on the Network World Technology Tour covering Mobility and Wireless (this week in Seattle and San Francisco).

Each week, I brought along a few different devices to try to find the best way to keep up with work and deadlines and still do all the time-intensive duties that this travel requires (attend trade show meetings in New Orleans and moderate the technology tour in four cities).

To say the experience was interesting would be an understatement. Even in 2005, being on the road can mean not having a high-speed network connection, although the options are more plentiful than ever before. Just be sure that your Internet connection works when you get into the hotel room (my Philadelphia room was wired incorrectly, which meant a technician needed to drop by to fix it).

Week 1: New Orleans

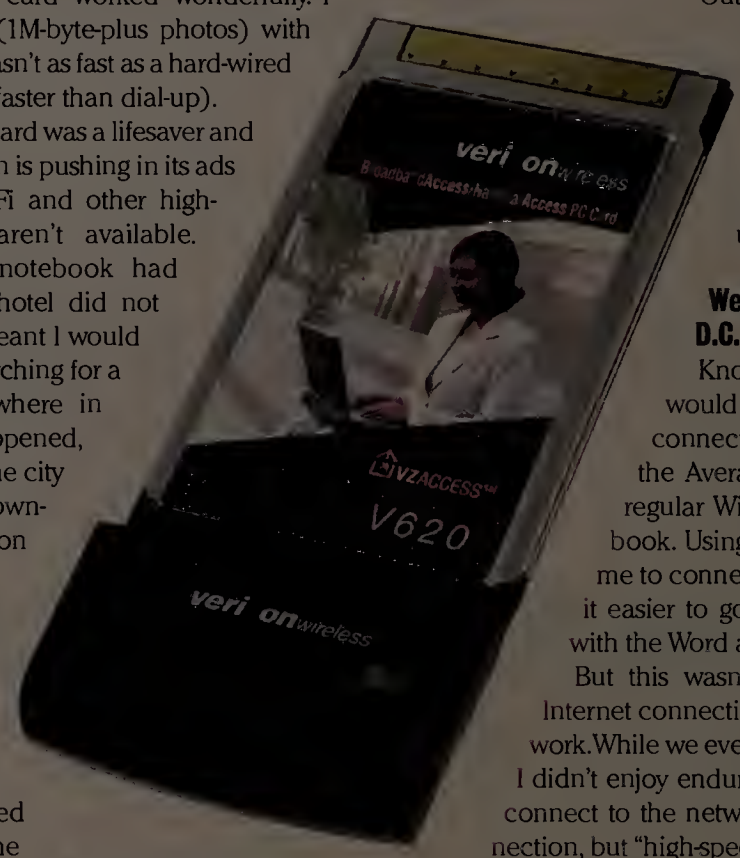
With a lot of hotels selling out quickly for the CTIA show, I had a suspicion that the hotel I was in would not have the wired high-speed Internet service, so I brought along a Verizon EV-DO PC Card (the V620) and connected it to an Averatec C3500, a convertible notebook that can double as a Tablet PC.

My suspicions were correct when I found myself in an interior hotel room (without windows) and no high-speed connection.

Thankfully, the V620 card worked wonderfully. I transferred large files (1M-byte-plus photos) with relative speed (it still wasn't as fast as a hard-wired connection, but much faster than dial-up).

In this case, the V620 card was a lifesaver and did exactly what Verizon is pushing in its ads — it works when Wi-Fi and other high-speed connections aren't available. While my Averatec notebook had embedded Wi-Fi, the hotel did not offer wireless, which meant I would have had to go out searching for a Wi-Fi hot spot somewhere in New Orleans. As it happened, the two days I was in the city there were torrential downpours, making that option less attractive.

The question becomes whether the card's cost and the wireless data service ($50 with rebates, plus $80 per month for unlimited data) justifies itself in the end. If I were a more frequent traveler I would say absolutely, but in my situation I feel that I don't travel enough for that cost (on average I travel only once per month; this stretch is unusual).



With this Verizon EV-DO PC card and a Verizon service agreement, I was able to enjoy broadband Internet access from a hotel room that lacked a high-speed connection.

The only glitch during Week 1 was that I didn't have Outlook or Microsoft Word installed on the Averatec notebook (evaluation units usually don't come with these applications loaded), which meant for e-mail I had to use the Web-based e-mail access and had to use WordPad to write my stories.

Week 2: Philadelphia; Washington, D.C.

Knowing that the Technology Tours would be in hotels with high-speed connections, I decided to not take along the Averatec notebook and brought my regular Windows 2000 Compaq Evo notebook. Using my regular notebook allowed me to connect to the company's VPN, making it easier to go through e-mail and file stories with the Word application.

But this wasn't all grins and giggles — the Internet connection initially in Philadelphia didn't work. While we eventually got it fixed, it was a hassle I didn't enjoy enduring. In Washington, I was able to connect to the network via a wired high-speed connection, but "high-speed" was a misnomer, as my connection speed resembled something closer to dial-up.

Week 3 now beckons, and I plan to bring both notebooks, as well as a couple of travel routers to see if my hotel broadband can provide wireless LAN connectivity so I can check e-mails while sitting on the bed or away from the desk. Stay tuned.

Shaw can be reached at kshaw@nww.com.

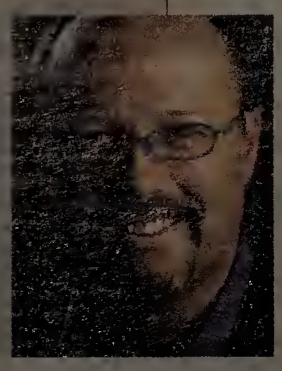
AT&T and Entenmann's Bakeries

Can your network make a really smart cookie?

ENTENMANN'S® BAKERIES AND AT&T. When the Bakers of Entenmann's wanted to make sure the shelves were stocked full with only the freshest product, they headed straight for the world's networking company. Now, with networking solutions from AT&T, Entenmann's Bakeries can receive detailed sales information from thousands of retail stores, utilize that information to identify the products needed, transmit the data to regional bakeries, and dispatch trucks to fill the shelves with fresh pastry even before it has a chance to cool. **CAN YOUR NETWORK DO THIS?**

AT&T
The world's networking company℠

To find out how AT&T's networking solutions helped Entenmann's transform its business, go to:
att.com/cookie



ON TECHNOLOGY

John Gallant

Vote off the weakest at N+I 'Survivor'

If you're a reality TV fan, you're going to love the special keynote presentation we're putting together for the upcoming NetWorld+Interop conference in Las Vegas.

In our "Survivor: Las Vegas" session, I'll be joined by an all-star cast of *Network World* columnists and test experts as we talk about which companies and technologies will thrive in the enterprise IT environment of tomorrow and which ones you — the buyers — will cast away.

The keynote panel is based on CBS' popular Survivor television series, and — as the show's motto states — we'll argue about which companies and technologies can outwit, outlast and outplay competitors to dominate the next generation of enterprise computing.

There will be no shrinking violets here: Panelists and audience members will vote off the providers and the technologies that just don't have the moxie to survive in your IT shop. They'll tell you who's smarter, faster and more wily, and who's too slow, too weak and too worried about the installed base to survive the major changes ahead — changes that include the virtualization of computing, storage and networks, and the move to services-oriented applications.

I'll be joined onstage by Paul McNamara, news editor and author of the 'Net Buzz column, and his back-page mate, Mark Gibbs, writer of our popular BackSpin and Gearhead columns. Also, we'll have Johna Till Johnson, who pens our Eye on the Carriers column, and Network World Lab Alliance stalwarts Joel Snyder, founder of Opus One, and David Newman of Network Test.

IT infrastructures and applications are changing rapidly — changes we're documenting in our New Data Center supplements — and you need to know which players and products will evolve and which will be left behind. My panelists cover the broad landscape of enterprise companies and technologies, and they won't be shy in telling you who's in a good position and who's at risk. You'll glean a wealth of information that will help you place smarter budget bets on strategic vendors and technologies.

We'll look at companies and products in the major program areas for the NetWorld+Interop conference. Those include: wireless; security; VoIP and collaboration; network infrastructure/services; performance; and data management/compliance.

We're slated for 5 p.m. on Wednesday, May 4. If you're not already booked for the conference, you can sign up at www.interop.com.

Who will stand tall? Whose torch will be extinguished? Share the fun and share your thoughts at "Survivor: Las Vegas"!

—John Gallant
Editorial director
jgallant@nww.com

opinions!

AT&T responds

Regarding Thomas Nolle's column, "AT&T: What went wrong?" (www.nwfusion.com, DocFinder: 6428): While Nolle is correct in saying the 1984 divestiture of the Bell companies resulted in a critical access problem for AT&T, he draws a number of inaccurate conclusions.

In suggesting AT&T should have vigorously pursued UNE-L over UNE-P in the years immediately following the Telecommunications Act of 1996, Nolle overlooks two important facts: 1) At that time, AT&T pursued its own alternative access with its AT&T Broadband division; and 2) since the passage of the act, FCC support for the Triennial Review Order remains razor thin, and the order was under incessant legal attack by the Bell companies.

These and other factors led us to conclude it made no sense for AT&T to invest significant capital in the Bells' last mile. The fact that the FCC has now modified the rules in such a way that neither UNE-L nor UNE-P is viable proves that AT&T made the right decision. The reality is, after we sold AT&T Broadband, utilizing UNE-P in the short term was the best way for us to offer a competitive bundle to customers.

As for Nolle's assertion that we abandoned our wireless and broadband strategies, he is ignoring the capital constraints that compelled this action. We had, at the time, a balance sheet saddled with $65 million in debt, billions of dollars in annual interest expense and declining cash flows from our core long-distance operations. AT&T would not have been able to fund the capital investments those businesses needed to pursue their own growth strategies. We certainly would have preferred to keep both our wireless and broadband divisions. Unfortunately, that was not an option.

With regard to AT&T CallVantage Service, we remain committed to its development and continue to roll out new innovations and features. Direct mail, advertising and traditional marketing cost our VoIP competitors more than $400 per new subscriber — a cost we found impossible to justify given the margins in the VoIP business. Instead, we have sought new and cost-effective distribution techniques. With the SBC merger, we believe we have found one.

Combining SBC, the leading wireless company, the second-largest local exchange carrier and an aggressive broadband deployer, with AT&T's leading enterprise IP networking business is a great outcome for our employees, customers and share owners. There is no denying consolidation of functions will lead job losses. However, the new focus on competing with cable companies, growing wireless, and expanding IP enterprise networking will create more jobs in the long run.

Paul Kranhold
Vice president, public relations
AT&T
Bedminster, N.J.

E-mail letters to jdix@nww.com or send them to John Dix, editor in chief, Network World, 118 Turnpike Road, Southborough, MA 01772. Please include phone number and address for verification.

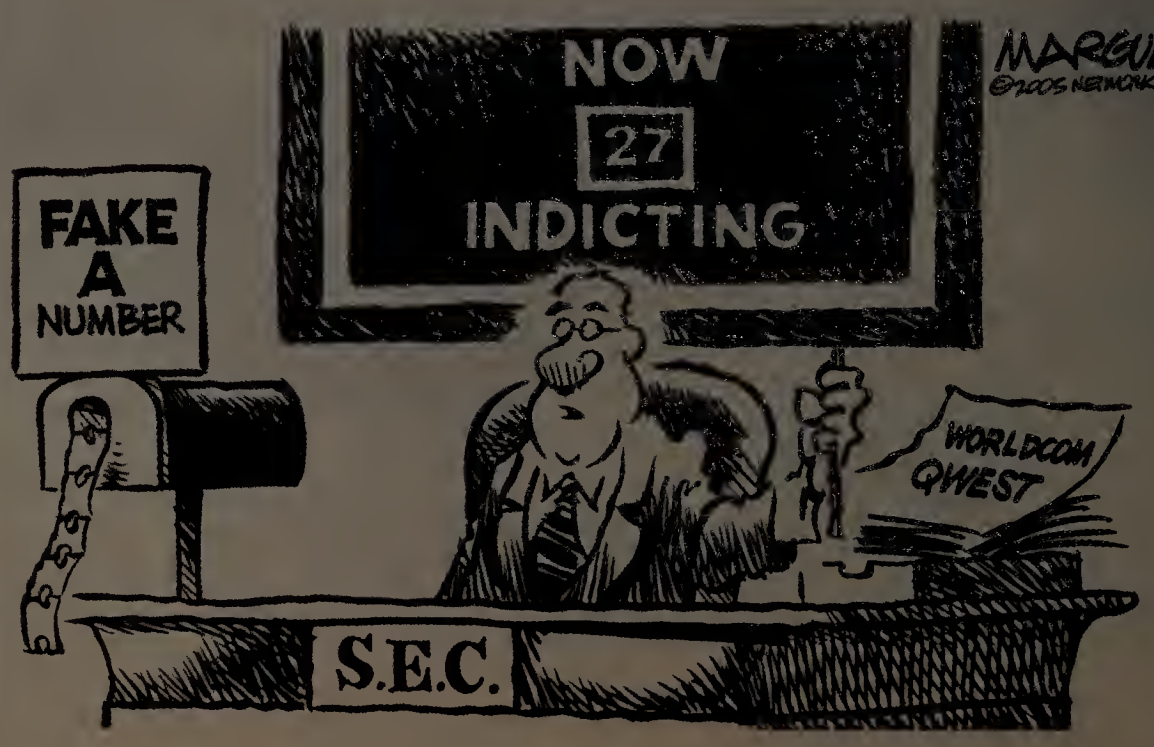
Not a Linux substitute

In his column "Novell: Long-term memory problems?" (DocFinder: 6429), Dave Kearns notes that Novell CEO Jack Messman said in his recent LinuxWorld keynote address that many of Linux's benefits "are due to a common code base from the desktop to the server to the data center." Kearns adds, "Well, if you remove the word 'Linux,' and substitute 'Windows,' it's just as valid a statement."

Windows isn't as homogeneous as Microsoft would have us believe. CE is wildly different from XP, which is wildly different from 9x/ME. Linux, on the other hand, truly does run on everything from watches to supercomputers with one code base.

Leon Brooks
Perth, Australia

More online! www.nwfusion.com Find out what readers are saying about these and other topics. DocFinder: 6427



INFRASTRUCTURE INSIGHTS

Dan Minoli

Is MPLS ready for prime time?

Many carriers are replacing their aging ATM WAN services with Multi-protocol Label Switching services. Carriers and equipment manufacturers virtually have stopped enhancing their ATM networks and equipment. Fortune 500 companies are considering incorporating MPLS services into their WANs.

Nevertheless, potential users have many questions about MPLS — questions that carriers should address explicitly and directly.

ATM was priced according to precise parameters such as port speed, sustainable cell rate and service type. How do carriers plan to charge for MPLS service? Based on maximum access/port speed only? Based on some kind of class of service (CoS) or differentiated service? Based on distance? Based on number or type of label-switched paths? How does one compare the cost of an ATM service with the cost of an MPLS service? When is one more cost-effective than the other? How does one compute total cost of ownership on an intranet using MPLS vs. ATM? How does a company financially justify migrating from one technology to the other? Carriers need to help users make the business case.

Carriers also should keep in mind that user companies want to lower their IT and telecom costs over time. Macro-level connectivity costs have been decreasing across the board at a rate of 10% to 20% per year for the past 10 to 15 years. An organization that has used an ATM network for five years or more might expect substantial cost advantages if and when it moves to MPLS. When carriers launched frame relay services in the early 1990s, they priced the services to be competitive with the cost of private lines, which is what made frame relay so successful throughout the 1990s.

Some IP purists prefer IP to MPLS. Can carriers shed some light on why MPLS might be preferable for heavy-duty core WAN applications over simple IP?

How does an MPLS network handle different classes of applications? What mechanisms are available to manage different CoSs, prioritization and QoS? ATM provided a number of service types with different service levels. What do carriers offer in this arena for MPLS?

How does the carrier handle oversubscription, "burstiness," traffic management, traffic shaping and overall end-to-end service metrics? Clearly ATM had a lot to offer here. What comparable mechanisms are available in carrier MPLS services?

Security is a major user concern, and encryption often is a must-have. How are security and encryption supported in MPLS? Will the provider equipment handle encryption directly — and if so, how will key distribution work? Or will the task be relegated to the customer equipment?

These are just some of the most fundamental questions users eager to road test MPLS should ask. After the carriers give clear, direct, straightforward answers to these questions, perhaps a dozen more queries will be posed and answered . . . and then we'll be ready to deploy MPLS in the enterprise.

Minoli is an adjunct professor in the Stevens Institute of Technology's graduate school and author of several books about enterprise networking. He can be reached at minoli@att.net.

Potential users have many questions about MPLS — questions that carriers should address explicitly and directly.

ON SECURITY

Winn Schwartau

It's time to redefine identity

"There is no such thing as electronic privacy. The essence of our very being is distributed across thousands of computers and databases over which we have little or no control. From credit reports to health records, from Department of Motor Vehicles computers to court records to video rentals, from law enforcement computers to school transcripts to debit card purchases, from insurance profiles to travel histories to our personal bank finances, everything we do and have done is recorded somewhere in a digital repository.

"The sad fact is that these very records which define us as an individual remain unprotected, subject to malicious modification, unauthorized disclosure or out-and-out destruction. Social Security Administration employees have sold our innermost secrets for $25 per name. Worse yet, as of today, there is nothing you can do to protect the digital you. You are not given the option or the opportunity to keep yourself and your family protected from electronic invasions of privacy.

"Your life can be turned absolutely upside down if the digital you ceases to exist. Electronic murder in cyberspace: You are just gone. Try proving you're alive; computers don't lie. Or if the picture of the digital you is electronically redrawn just the right way, a prince can become a pauper in microseconds. In cyberspace, you are guilty until proven innocent."

I first wrote these words in my 1991 book *Information Warfare* (free online at www.nwfusion.com, DocFinder: 6432), and they are still disturbingly true. According to the Better Business Bureau's (BBB) 2005 Identity Fraud Survey Report (see DocFinder: 6433), the identity theft problem is improving significantly. But that's small consolation to the 9.3 million victims in 2004 (down from 10.1 million in 2003) that cost our economy a staggering $52.6 billion last year.

What causes the majority of ID theft cases is sheer stupidity. The solution to ID theft is sheer simplicity.

Despite global reliance on e-commerce, we still take a 1930s approach to identity management, with Social Security numbers (SSN) our de facto national identification. Knowledge of name, address, credit card and SSN — all publicly available information — is still all that is required to establish a legally binding means of personal authentication. Congress' shortsighted E-Sign bill of 2000 compounded the problem instead of raising the security bar.

The BBB Identity Fraud Survey shows that only 11.6% of ID theft cases occur online. The rest comes from traditional offline physical means: lost ID, checks, credit cards, stolen mail and dumpster diving. Yet we still rely on static data as ID proof positive. What to do?

We need to legally redefine what we mean by "proof of identity." We should employ rigorous two-factor identification through real-time handshaking to establish identity to a higher standard. Whether it is a smart card with password, a time-based token or some form of biometric ID, anything is superior to today's dangerous relic.

Congress should not try to legislate 21st century life with 1930s technology. It should instead recognize that the nature of legal identity has so radically changed it must be redefined to thwart the ease of ID theft.

This is not a new problem. Our government chose to ignore it, thus creating a multibillion-dollar crime syndicate that easily disrupts citizens' lives. We all pay the price with higher prices and interest rates, and loss of productivity. This is sheer insanity, especially when the answer has been readily available for 15 years.

Will any ID theft solution be perfect? No. Will someone always find a way around the system? Yes. Is raising the security bar a good step? Always. To try to fix past errors by making the same mistakes over and over is sheer insanity. Let's give sheer simplicity a try. We have the technology. We can fix this problem.

Schwartau is a security writer, lecturer and president of Interpact, a security awareness consulting firm. He can be reached at winn@thesecurityawarenesscompany.com.

What causes the majority of ID theft cases is sheer stupidity. The solution to ID theft is sheer simplicity.

NEW TOOLS QUANTIFY VoIP CALL

Management applications measure packet loss, jitter and latency to zero in on problems plaguing converged networks.

■ BY SUSAN BREIDENBACH

Do you trust a computer to tell you how your CEO's new IP phone sounds?

Network testing and monitoring vendors are betting you will as they peddle new call quality management applications that pinpoint problems on converged networks. Despite increasing reliance on e-mail, voice remains executives' method of choice for closing deals, and businesses embracing VoIP can't afford to make assumptions about call quality.

Vendors such as Apparent Networks, Brix Networks, Empirix, Integrated Research, Qovia and Spirent are rushing to fill the void, often licensing algorithms for active testing and passive monitoring from call quality pioneers Psytechnics and Telchemy. "This is the beginning of a big push, though the standards for VoIP call quality measurement are still evolving," says Eric Siegel, senior analyst at Burton Group.

Frost & Sullivan reckons the emergent VoIP monitoring/management market hit $50.7 million in 2004, and expects it to increase about sixfold by 2008. IP telephony is exploding, and upfront network assessments will only take a VoIP implementation so far. Unlike data, it has to work perfectly out of the gate.

"VoIP can be made to run as well and as reliably and as clearly as the best traditional phone network, but it's not a static environment," says Pierce Reid, vice president of marketing for Qovia, a 3-year-old start-up dedicated to VoIP call quality. "It has entropy. This can be accelerated by the employee who decides to download 'Shrek 2' at lunchtime."

Keeping the canaries singing

Network professionals with converged environments liken IP telephony to the cages of canaries that used to accompany the miners below ground. The birds keeled over when conditions in the mine became unsafe. Voice is revealing network problems that used to go unnoticed on IP networks, and the standard data fix — more bandwidth — doesn't work.

"These real-time applications are showing us we have problems on the network end to end," says Walt Magnussen, director of telecom at Texas A&M University in College Station, which uses Apparent's AppareNet Voice software probe to support VoIP and video links to remote locations. "This new tool shows you where it is and what it is."

VoIP call quality management includes active and passive approaches, and particular products can encompass both. The active or intrusive approach is exemplified by British Telecom spinoff Psytechnics with its algorithms derived from years of subjective voice-quality testing. The method includes installing a thin client on various endpoints — such as phones, gateways and call servers — to take local readings and return a Perceptual Evaluation of Speech Quality metric.

"You insert a reference signal at one point, measure it at the destination, and through the use of algorithms calculate what the Mean Opinion Score would be," says George Hamilton, senior research analyst at The Yankee Group. "It's an active test, and it's more accurate." MOS is a metric of how good a voice call sounds (see story, below).

This intrusive method allows for very targeted testing of specific network links and elements. The measurement goes end to end and establishes a baseline for comparison. Among the weaknesses, the simulated traffic eats up network bandwidth. Also, intrusive testing can be difficult when you don't control the entire path from one end to the other.

Telchemy championed a passive, non-intrusive approach that produces voice quality metrics extrapolated entirely from network statistics such as packet loss and jitter. The company's VQmon technology has been embedded in a range of third-party IP phones, gateways, probes, analyzers, switches and routers to enable real-time monitoring of VoIP call quality.

AppareNet Voice has been described as a hybrid of the non-intrusive and active approaches. The product generates test traffic and then uses software probes to listen to it, but doesn't require the

Voice quality standards

The legacy voice quality standard is the Mean Opinion Score. A MOS is derived by having people rate the quality of test sentences read aloud over the same communications circuit by male and female speakers. Each sentence is assigned the score of (1) bad, (2) poor, (3) fair, (4) good or (5) excellent, and the scores are averaged.

This expensive, labor-intensive process is reserved for laboratory settings, with no real-time applicability. The MOS scoring is also highly subjective; different listeners might rate the same sentence at opposite ends of the scale.

The industry turned to computers for consistency and economy, and the Perceptual Evaluation of Speech Quality (PESQ) algorithm was co-developed by KPN/TNO and Psytechnics and formalized as ITU P.862. PESQ measures the distortion of test voice signals as they move through a VoIP network and estimates a MOS. While this works fairly well, PESQ sometimes gives high marks to poor signals, and low marks to conversations that sound just fine to human listeners.

Also, PESQ is for active monitoring, and as such is intrusive. The newer ITU P.563 standard, like Telchemy's proprietary VQmon technology, is for non-intrusive monitoring of voice streams. This passive approach lets call quality be estimated as conversations occur.

The ITU also established G.107, commonly known as the E Model. This model considers the mouth-to-ear characteristics of a given speech path and assigns an R value between 0 to 100, although the practical range for the ubiquitous G.711 codec is 50 to 94. The actual formula is R = Ro − Is − Id − Ie + A, where

- Ro is a base factor determined from loudness.
- Is are impairments that occur simultaneously with speech.
- Id are impairments that are delayed relative to speech.
- Ie is an equipment impairment factor.
- A is an advantage factor.

The E Model is a scalable, lightweight protocol for making repeated measurements throughout the call.

Voice quality adds a new dimension to network management. The IETF addressed VoIP management with RTP Control Protocol Extended Reports (RTCP XR), a protocol that can be implemented inexpensively via software in IP phones and gateways. RTCP XR measures call quality using such key metrics as packet loss and discard; delay; signal, noise and echo levels; and configuration data. These metrics can be sampled midstream by a probe or analyzer, or an SNMP system can collect them from a gateway.

— Susan Breidenbach

VoIP REPORT

QUALITY

installation of appliances or software agents at the remote sites.

"You just need to know the IP address at the other end, and you can do hundreds of sites an hour," says Gary Audin, president of Delphi, a network integrator in Arlington, Va. "Once you have to start putting agents in all the remote locations, it's a much bigger undertaking."

The remote locations in Texas A&M's VoIP network include extension facilities and experimental agricultural sites in Latin America, Africa and the Middle East. To help serve such areas, the university, an official Internet2 Technology Evaluation Center, also is working with the American Distance Education Consortium (ADEC) at the University of Nebraska and satellite provider Tachyon Networks on the prioritization of VoIP traffic over satellite links.

Texas A&M recently used AppareNet Voice to assess the voice capability of a link with an agricultural research center in Kenya, which starts with a terrestrial gateway connecting the U.S. and Europe and then moves onto a satellite link for the rest of the trip. The tool pinpointed a software problem in the infrastructure of the satellite provider, which could not come up with a cost-effective fix, forcing Texas A&M to look for an alternate carrier.

However, the university had better luck with the ADEC trials testing a path involving a satellite link out of San Diego, serving locations in Latin America. AppareNet Voice found a problem with a router, Tachyon replaced it, and the connection now supports VoIP.

AppareNet Voice sends out several hundred packets of various types to each router along the way and then uses the returning information to characterize the link and assess any problems.

"With this kind of tool, I can look into another carrier's network in a fairly non-intrusive fashion, without installing any software anywhere else," Magnussen says. "It's hard evidence for the vendor or service provider. The measurements aren't precise, but heck, for something you can come up with on demand in 4 or 5 minutes — it's pretty good."

Others feel the value of local appliances or agents throughout the network is worth the upfront time and expense. Apptis, a large network integrator in Chantilly, Va., uses the Qovia VoIP Monitoring and Management System internally and in VoIP implementations for clients.

"What struck us was its ability to do real real-time monitoring," says Mark Melvin, a senior solutions engineer at Apptis. "Qovia is monitoring the actual traffic stream, vs. looking at the call detail reports after the fact."

Melvin also applauds Qovia's distributed architecture. There is no agent running on the Cisco Call Manager server, which simplifies troubleshooting when a Call Manager process causes the problem. If an alert threshold is hit during a call, the troubleshooting can start before anyone complains.

The Qovia ION appliances can be software-upgraded remotely, and the reboot process is fairly quick. If the central Qovia server is brought down for maintenance, the remote appliances can continue to gather information and will report it as soon as the server comes back online.

"With the new scaled down ION appliances, Qovia becomes a much more scalable and cost-competitive solution to distribute across your entire environment, making it competitive with some software-only solutions," Melvin sums up.

CHARTING CALL QUALITY

This typical representation of call quality levels shows what E Model R factors and MOS scores make for good and bad phone.

THE E MODEL: ITU G.107 considers the mouth-to-ear characteristics of a given speech path and assigns an R value between 0-100.

E model:
R = Ro - Is - Id - Ie +A

- Ro is a base factor determined from loudness.
- Id is the impairments that occur simultaneously with speech.
- Id is the impairments that are delayed.
- Ie is the effects of equipment impairments.
- A is the advantage factor to account for caller's expectations.

MEAN OPINION SCORE (MOS): MOS is a numerical representation of voice quality derived by having a pool of listeners rate a series of audio files. An average score is then calculated.

User Opinion	R Factor	MOS Score
Maximum obtainable for a G.711 codec	93	4.1
Very satisfied	90-100	4.1-5.0
Satisfied	80-90	3.7-4.1
Some users satisfied	70-80	3.4-3.7
Many users dissatisfied	60-70	2.9-3.4
Nearly all users dissatisfied	50-60	2.4-2.9
Not recommended	0 - 50	1.0-2.4

SOURCE: TELCHEMY

The cost of quality

Voice quality testing and monitoring don't come cheap, which is one reason the vendors have, with few exceptions, focused on the service providers, testing laboratories and big integrators up until now. Some of the new enterprise-scaled products start in the $30,000 to $40,000 range.

"You can pay that much for a one-shot network assessment service, or buy our The Hammer VoIP Test Solution for Enterprises bundle and have it to use again," counters Jeff Fried, CTO for Empirix, which introduced its first enterprise-targeted products at VoiceCon last month.

Call center UpSource uses the Empirix product to test the stations of remote call center agents using softphones. UpSource CTO Mark Burns says he wanted something that could continually make assessments so new VoIP applications and VoIP capacity could be added on demand.

"We are in the business of solving customers' problems, so we can't have lots of complaints about voice quality as we move into convergence, any more than we can have lots of down time," Burns says. "These tools are important for the same reason that network redundancy is extremely important."

Qovia tells prospective customers that they can expect a good VoIP call quality management product to add 10% to 20% to the cost of a new VoIP system, and Melvin of Apptis says it is worth the premium. "The businesses that understand the value of network management will understand the importance and necessity of these tools. As you move from traditional to IP telephony, there are a lot more pieces to manage," he says.

Initial customers tended to seek out VoIP call quality products in desperation, after an implementation had already gone bad. However, vendors detect a shift.

"We're starting to see more traction with new installations," says Nick Orolin, a vice president at Integrated Research, maker of Prognosis for IP Telephony for the Cisco environment. "Enterprises are budgeting for VoIP management upfront and bundling it in with initial deployments."

VoIP REPORT

Big voice-equipment manufacturers such as Nortel are bundling call quality management into their VoIP platforms as well. Erlanger Health System, which started migrating its five-site Nortel shop to VoIP in 2001, quickly saw the value of enhancements in the Succession 3 switch that could feed jitter and packetization statistics and other key VoIP call characteristics into Nortel's Optivity Telephony Manager.

With these tools, a more voice-oriented stress test could be done before upgrading another group of phones to VoIP. "We get a good call quality baseline upfront, instead of just sticking a bunch of phones out there and then seeing what problems we encounter," says John Haltom, network director for Erlanger, a public teaching hospital affiliated with the University of Tennessee School of Medicine in Chattanooga.

Now on the Succession 4 IP PBX platform, Erlanger has begun a trial of the call- quality testing and monitoring capabilities in Nortel partner NetIQ's AppManager 6.0. Tapping into enhancements in the Succession 4 server and Phase 2 IP phones, AppManager 6.0 can provide deeper information about calls in progress.

"Now testing and monitoring technology is embedded in the phone itself, and the phone can report to the switch whenever it has an issue," Haltom says.

Erlanger has migrated 900 of its 1,300 desktops to IP phones, and 800 of them are Phase 2 models that contain the necessary processing power, RAM and software to participate in this type of proactive management.

"A lot of organizations can probably get by without proactive call quality management, but we are a hospital, so we have to plan for the worst and engineer our network a bit differently," Haltom says. "NetIQ's AppManager 6.0 is a true enterprise-wide network management platform that looks at voice quality management with the help of the switch and the phones, and reports alerts in any way that meets your needs."

A self-healing future?

Once VoIP call quality monitoring systems are in place, it is tempting to speculate about what a little artificial intelligence might add to the mix.

The idea would be to incorporate some expert systems technology into the solution and make VoIP networks self-healing. The gateways could take the call quality information and use it to move traffic around to the more optimal paths.

However, the cultural hurdles might be bigger than the technological hurdles.

"Integrated Research actually supports some very interesting automation, and a lot of people express an interest in the self-healing concept," Orolin says. But in the final analysis, no one is willing to stick their necks out and actually implement it and trust it. "I think rules-based automation is a good five years off."

Breidenbach is a freelance writer in Nevada. She can be reached at sbreide@aol.com.

LISTEN UP

Hear the distinction between various levels of voice quality on Network World Fusion. There you'll find audio samples provided by Telchemy that offer a comparison of MOS scores ranging from 1.0 (poor quality) to 4.1 (toll quality).

www.nwfusion.com, DocFinder: 6426.

Manage your data center from anywhere...

In today's pressure filled "uptime" environment where a few minutes can cost you big dollars, customer confidence and worker productivity, you can't afford to have IT problems. And, you know fewer administrators and "lights out" control of your data centers gives you a much-needed security buffer.

Lantronix gives you access to ALL of your data center assets from anywhere over the Internet via a browser, and total out-of-band access if the network is down. We also offer the only console manager available with a NIST-certified implementation of Advanced Encryption Standards (Rijndael)† along with SSL and SSH – assuring you the highest level of security available.

SecureLinx™

Lights out remote data center management.

Secure Console Managers

Remote management of Linux, Unix and Windows® 2003 servers, routers, switches, telecom and building access equipment.

- Respond faster and reduce downtime
- Consolidate resources and minimize costs

Remote KVM™ via IP

Manage an entire room full of Windows and Linux servers from a single desktop, from anywhere over the Internet.

- Eliminate need for multiple keyboards, monitors and mice
- No client software required

Remote Power Managers

Control the power, individually, to every device in the data center via a web browser.

- Reboot system remotely
- Ensure safe power distribution and reduce in-rush overload

Network Computing Editor's Choice

SecureLinx SLC16
Winner of the Network Computing Editor's Choice Award

LANTRONIX®

Network anything. Network everything.

†As of August 2004, SecureLinx SLC is the only console manager with a NIST-certified implementation of Advanced Encryption Standards as specified by FIPS-197 (Federal Information Processing Standards).

www.lantronix.com | (800) 422-7055

There's nothing standard about our industry-standard servers.

Intel® Pentium® 4 Processor power and the features you need—now at about the price of a desktop PC. The HP ProLiant ML110 server has rich features like two 80GB ATA Drives and an embedded PCI Gigabit NIC. That means it's ready to handle your storage and performance requirement needs. Yet the ML110 is in the same price range as less well-equipped competitors' boxes. And these aren't just features for features' sake. They are designed to improve the reliability, performance and expandability that growing small and medium businesses require. Add DAT 40 to help solve your storage and backup issues securely and affordably. These are just two HP Smart Office solutions that give you more expertise, technology, service and support. Raise your standards, not your budget.

HP ProLiant ML110 SERVER

$849 Lease for as low as $24 a month[4]

$189 Savings[1] ($1,038 - $189 = $849)

- Intel® Pentium® 4 Processor (3E GHz/800MHz FSB)[2]
- 512MB Advanced ECC PC3200 DDR SDRAM
- Embedded Dual Channel Ultra ATA Controller
- Two 80GB ATA hard drives
- Embedded PCI Gigabit NIC
- Hardware limited warranty, 1-year parts, 1-year labor, 1-year on-site support[3]

HP Care Pack: $149
Next-day on-site coverage for $1 per week for 3 years.

Add secure backup.

HP StorageWorks DAT 40 TAPE DRIVE

- 40GB (compressed) per tape
- 6MB/s transfer rate (compressed)
- Includes One Button Disaster Recovery for quick service restores
- 3-years parts exchange; next-business-day response

$699 Lease for as low as $20 a month[4]

MORE ADVICE | MORE TECHNOLOGY | MORE SUPPORT

Download *How Do I Choose A Server?*
Our free guide answers your questions.

CALL	**1-800-888-5907**
CLICK	**hp.com/go/ML110mag2**
VISIT	**your local HP reseller**

hp invent

intel inside pentium 4

Prices shown are HP Direct prices; reseller and retail prices may vary. Prices shown are subject to change and do not include applicable state and local taxes or shipping to recipient's address. Offers cannot be combined with any other offer or discount, are good while supplies last and are available from HP Direct and participating HP resellers. All featured offers available in U.S. only. 1. Savings based on HP published list price of configure-to-order equivalent. 2. Intel's numbering is not a measurement of higher performance. 3. Certain warranty restrictions and exclusions may apply. For complete warranty details, call 1-800-345-1518 (U.S.). 4. 48-month implicit lease rate, assuming lessee does not exercise a fair-market-value purchase option at the end of the lease term and timely returns the leased equipment to Hewlett-Packard Financial Services Company (HPFSC) at the end of the lease term and disregarding any charges payable by lessee other than rent payments (such as taxes, fees and shipping charges). Leasing valid through 4/30/05 on all lease transactions with a total transaction amount between $349 and $150,000. Intel, Intel Inside, the Intel Inside Logo and Intel Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

CLEAR CHOICE TEST

VoIP analysis tools

Picking up VoIP-specific tools for the network management workbench

■ BY EDWIN MIER, DAVID MIER AND ROBERT TARPLEY, NETWORK WORLD LAB ALLIANCE

Some cavalierly refer to IP telephony as "just another application" that rides over your data network. But wait and see what happens if VoIP call quality starts eroding or, worse yet, if your organization's phone calls stop altogether.

In this Clear Choice Test, we evaluated a burgeoning class of new products, collectively called VoIP analysis tools. These wares help the VoIP network manager proactively monitor and troubleshoot the IP telephony environment to ensure call continuity.

Seven vendors accepted our invitation: Agilent Technologies, Brix Networks, ClearSight Networks, Fluke Networks, Touchstone Technologies, Viola Networks and WildPackets.

ClearSight's Analyzer garnered the Network World Clear Choice award for its extreme ease of use and its capability to analyze a range of VoIP protocols. Fluke's OptiView package made a strong second-place showing by capturing a substantial amount of information on the VoIP calls. However, it was a bit more tedious to use. There was a near-three-way tie for third place between Agilent, Touchstone and WildPackets, all of which provided much more complete analysis of VoIP traffic in the Session Initiation Protocol (SIP) environment than proprietary environments.

Protocols matter

We found — and users also need to keep in mind — that VoIP analysis tools are oriented toward particular VoIP protocol environments. Interpreting different call-control-protocol sequences is difficult because the messages vary considerably with the particular protocol used.

We tested each package in four different VoIP environments over a two-month period (see "How we did it," page 52). Using this methodology, we tested the packages against three proprietary protocols and with two SIP-based implementations.

VoIP REPORT

The tools tested dramatically differ in their abilities to monitor and track SIP standards-based VoIP activity compared to how they work in proprietary protocol environments. Only two of the products, ClearSight's Analyzer and Fluke's OptiView package, did a good job tracking all VoIP activity in both standard-based SIP and proprietary-protocol VoIP environments.

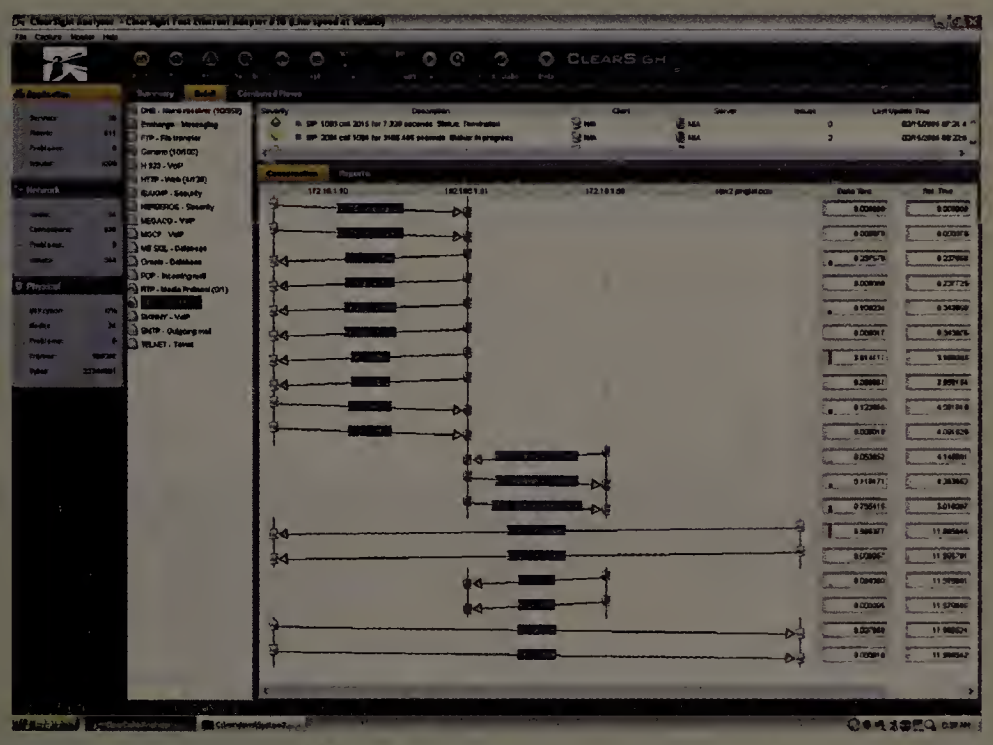
But other products tested — such as Agilent's combination of Distributed Network Analyzer MX (DNA MX) probe and Telephony Network Analyzer (TNA) software and WildPackets' EtherPeek VX — still can view parts of VoIP phone traffic in different protocol environments. This is because actual VoIP conversations follow a fairly standard format across protocol environments. They comprise bidirectional Real-Time Transport Protocol (RTP) over User Datagram Protocol (UDP) streams, which are fairly easy to spot and decipher using tools that recognize RTP streams even if the IP PBX uses a proprietary signaling protocol.

Plugging in

The tools we tested mostly are specialty PC-based software applications. Many are add-ons to the vendors' network data analyzer, which provide the ability to recognize and process IP-telephony call control and VoIP conversations.

Long-time test-and-monitor vendor Agilent addresses VoIP monitoring through Real-Time Transport Control Protocol and RTP monitor applications that integrate with its popular Network Analyzer package. Its VoIP analysis package can be based on a laptop, run off a mirrored switch port or run on a probe appliance inserted in-line in key backbone network segments. We tested Agilent's 100M bit/sec capacity DNA MX probe that can fit with almost any network interface type, handle Gigabit links at wire speed and be accessed remotely from anywhere on the network. We ran the TNA software on a separate PC that communicated with the DNA MX over the network.

We ran ClearSight's software-only Analyzer on a Windows XP laptop. It sniffs passing traffic and captures all the packets traveling on the network, then analyzes them for VoIP traffic and associates the VoIP packets with the proper conversation. The network analyst's laptop usually is situated on a mirrored switch port to watch traffic that's copied and redirected from key traffic links.



Driving ClearSight Networks' Analyzer: ClearSight gets high marks for its interface because all of its VoIP data and measurement can be accessed by applets from a single screen. VoIP streams are presented in log-type tables, with the ability to drill down for detail. A summary tab shows totals for bandwidth and flows and only a single click is needed to capture and playback any VoIP stream.

Fluke's OptiView package can run on a PC or on a special probe designed for in-line insertion on a backbone link and is based on packet-sniffing data capture and analysis. We tested it with a Gigabit-capacity in-line probe that cost about $21,800. We also ran it on a Windows 2000 laptop via a mirrored switch port. The VoIP analysis software was the same in both configurations, but the separate-probe approach is better suited to multi-site distributed environments.

Another implementation based on packet sniffing is Touchstone's software-only product, WinEyeQ, which we ran on a Win 2000 PC as it watched passing traffic on a mirrored switch port. WinEyeQ seems to be more focused on VoIP traffic than its packet-sniffing competitors because all of the screens in Touchstone's product were specifically designed for VoIP analysis.

WildPackets' EtherPeek VX is also Windows-based software and is a packet-sniffing monitor tool, which we ran on a Win 2000 PC, on a mirrored-switch-port connection.

Brix's BrixMon relies on hardware probes called verifiers that generate simulated VoIP traffic based on canned tests that you can tailor to your network. This test traffic is sent between verifiers. Brix says the system can monitor and report on real VoIP traffic, but we found it difficult to get this feature to work properly in the different scenarios.

Viola's NetAlly is a software-only package that also issues simulated streams of VoIP traffic sent between its distributed PC clients.

With simulated traffic there is no direct observation or monitoring of real user's VoIP traffic, therefore both BrixMon and NetAlly are indifferent to VoIP protocols. This can be useful if you plan to use the tool in a pre-deployment phase of an IP PBX system to assess if the current net-

VoIP REPORT

work infrastructure can perform adequately for VoIP traffic. But then, when real VoIP traffic is implemented on the network, you don't get the same level of VoIP-level protocol detail and real traffic analysis that the other packages provide.

In this category, our top marks went to Agilent and Fluke in large part because of the additional deployment topologies and options they support. The BrixMon system was notably much more difficult to deploy and get working properly.

Real-time VoIP monitoring

Our test is weighted heavily toward how well these products assist the process of real-time VoIP monitoring. Our assessment is based on whether information could accurately be reported in the following areas:

- VoIP call control (that is, call initiation and setup signaling).
- Status of current VoIP calls.
- Details about current VoIP calls (caller destination, vocoder used, etc.).
- Bandwidth consumption by current VoIP calls.
- IP addresses of key VoIP nodes and endpoints (call controller, gateways, IP phones).
- Latency, jitter and packet loss, for VoIP calls between two distributed sites.

The tools that offer real-time information turned in the best results, by far, when monitoring SIP-based VoIP activity. WildPackets did the best job, in part, because of its slick, graphical, state-based, SIP call-progress display. ClearSight was a close second, offering the same amount of real-time information. However, it wasn't as easy to determine which calls were completed. Agilent, Fluke and Touchstone all did a fairly good job tracking SIP-based call control.

Viola offers little in terms of in real-time monitoring and analysis of SIP or proprietary VoIP environments. Brix generates simulated VoIP protocols streams, too, like Viola, but also can monitor user VoIP streams to some extent.

When you turn to tracking proprietary call-control environments, ClearSight was the hands-down winner. In addition to the half-dozen VoIP protocols it formally supports, ClearSight categorized calls based on other proprietary protocols as generic call control. Fluke, which we placed second in this regard, did a good job tracking the proprietary call-control protocols, which classified them as "unknown" call control. ClearSight displayed the key VoIP parameters on one screen, where Fluke required additional windows to view all the parameters associated with a VoIP call.

How about tracking and reporting of VoIP calls? In the SIP environment, WildPackets had the best showing because you can click on a VoIP call and bring up a well laid-out display window showing a jitter graph, the server name, the IP addresses or the endpoints, and other call information. Agilent's tool set was also noteworthy. It displayed the VoIP calls on a tabular screen with the call information spread across the columns of the table.

Fluke and Touchstone reported similar information, but we felt it was more difficult to navigate the screens to view the data with these tools. ClearSight presented the VoIP statistics in a large table making it a bit tedious to find key VoIP parameters.

For call monitoring in proprietary-protocol environments, ClearSight and Fluke turned in good performances by still presenting all the VoIP call information. WildPackets and Agilent did an adequate job monitoring proprietary-protocol calls because of their general data-analysis capabilities, but none of the others could effectively display VoIP call information in proprietary environments.

The ability to report VoIP bandwidth consumption was also split along protocol lines. ClearSight did the best job accurately reporting VoIP bandwidth and other VoIP-activity details such as jitter, latency and packet loss in both the SIP and proprietary environments. Fluke was a close second here, effectively reporting VoIP details in all protocol environments but not as elegantly as ClearSight.

Based on SIP traffic only, Touchstone, Agilent and WildPackets all did an excellent job analyzing VoIP call control and reporting call performance statistics.

Across all protocols, Fluke did the best job monitoring and reporting key QoS conditions. ClearSight, Viola and Brix also did well monitoring QoS in all protocol environments, but there were some cases in which all information was not reported consistently. Brix and Viola reported QoS conditions based on their own generated traffic and were not sensitive to the actual VoIP control protocol used by the IP PBX.

In standard SIP-only environments, WildPackets and Fluke did the best job reporting network impairments and QoS-type conditions consistently and accurately. All other products displayed the QoS parameters, but, in some cases, the values were not reported consistently.

See VoIP, page 52

Net Results

ClearSight Analyzer 4.0

OVERALL RATING **4.7**

Company: ClearSight Networks, www.clearsight.com. **Cost:** $8,000 for all software. **Pros:** Supports standard and proprietary VoIP call-control protocols; best layout and easiest to use; displays both overall VoIP bandwidth and specific call bandwidth; excellent RTP replay capability. **Con:** Summary stats of VoIP activity could be improved.

NetworkWorld CLEAR CHOICE

Fluke OptiView VoIP, Protocol Expert Plus and Link Analyzer 6.1

OVERALL RATING **3.9**

Company: Fluke Networks, www.flukenetworks.com. **Cost:** From $6,700 for software; $21,795 for Gigabit-capacity probe appliance. **Pros:** Supports many deployment topologies; effectively monitors proprietary VoIP protocols. **Cons:** Tedious interface; easy to confuse monitor and capture modes, which yield different stats.

EtherPeek VX 1.0

OVERALL RATING **3.65**

Company: WildPackets, www.wildpackets.com. **Cost:** $10,000 for software. **Pros:** Super peer map features shows all active VoIP connections; clear breakdown of active vs. closed VoIP calls. **Cons:** Sees only SIP and H.323-based VoIP activity; displays are generally clear but static, not customizable.

Agilent DNA MX and TNA software 4.5

OVERALL RATING **3.55**

Company: Agilent Technologies, www.agilent.com. **Cost:** $20,000 for central server; $7,700 for TNA software. **Pros:** Supports many LAN/WAN interfaces; scales well across multiple sites, distributed topologies. **Cons:** Hard to maneuver around main VoIP table; poor online help; hard to interpret data in some instances.

WinEyeQ 1.3.5

OVERALL RATING **3.4**

Company: Touchstone Technologies, www.touchstone-inc.com. **Cost:** From $6,500 for all software. **Pros:** Excellent alerting; easy to set up, use; VoIP screens are well organized. **Con:** Sees only SIP and H.323-based VoIP activity.

BrixMon 2.1

OVERALL RATING **2.7**

Company: Brix Networks, www.brixnet.com. **Cost:** $31,000 for central server package; $1,800 to $7,500 per probe/site. **Pros:** Best for long-term status monitoring in large networks; reports many telephony metrics that others don't. **Cons:** Most complex system to set up and tedious use; not oriented to assessing individual VoIP calls.

NetAlly RealTime and VoIP Assessment 4.8

OVERALL RATING **2.45**

Company: Viola Networks, www.violanetworks.com. **Cost:** $12,500 for base software with five agents. **Pros:** Special tool for Cisco VoIP reporting; very good for pre-VoIP deployment network analysis. **Con:** Doesn't monitor or assess real user VoIP traffic.

The breakdown	ClearSight Analyzer	Fluke OptiView VoIP, Protocol Expert Plus, and Link Analyzer	WildPackets EtherPeek VX	Agilent DNA MX and TNA	Touchstone WinEyeQ	Brix BrixMon	Viola NetAlly RealTime and VoIP assessment
Real-time VoIP monitoring 40%	5	4.5	3	3.5	3	2	1
Usability; data clarity, navigability 30%	5	3.5	4.5	3.5	4	3	3.5
Configuration and deployment 10%	4	4.5	4	4.5	4	2.5	4
Reporting (alerts, MOS) 10%	4	3	3.5	3.5	3.5	4	3
Special & unique features 10%	4	3	3.5	3	2.5	3.5	3
TOTAL SCORE	4.7	3.9	3.65	3.55	3.4	2.7	2.45

Scoring key: **5:** Exceptional; **4:** Very good; **3:** Average; **2:** Below average; **1:** Consistently subpar

IP Telephony Switching Wireless Routing Security

Challenge 3Com®...

...to give you enterprise-class networking at an affordable price.

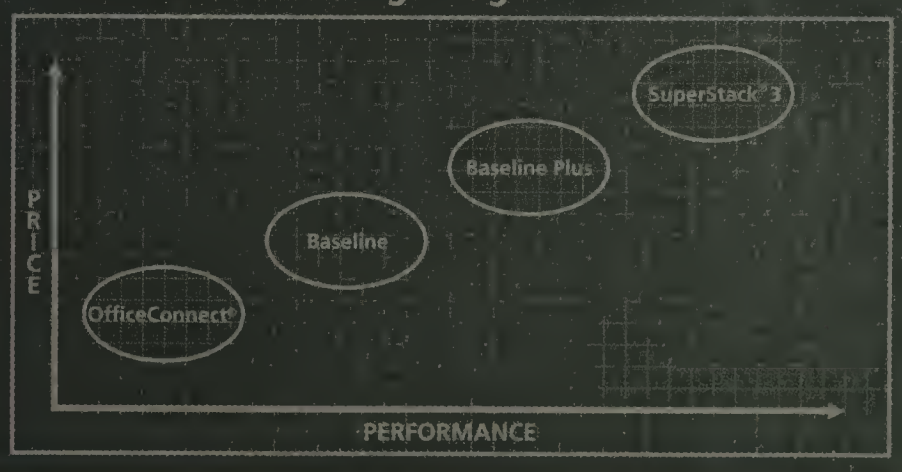
Challenge away – you'll find that no one else can offer you true enterprise-class performance at 3Com prices.

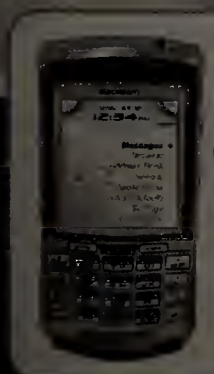
With advanced features like traffic classification and management, lifetime warranties with hardware replacement, plug-and-play installation and full interoperability, 3Com can give you radical performance and efficiency advantages at prices you can afford.

And now with prices on our renowned switches reduced by as much as 31%, you get even more performance for your money.

Ask your reseller about affordable enterprise networking and you'll find there's only one choice – 3Com.

3Com Value Switching Range



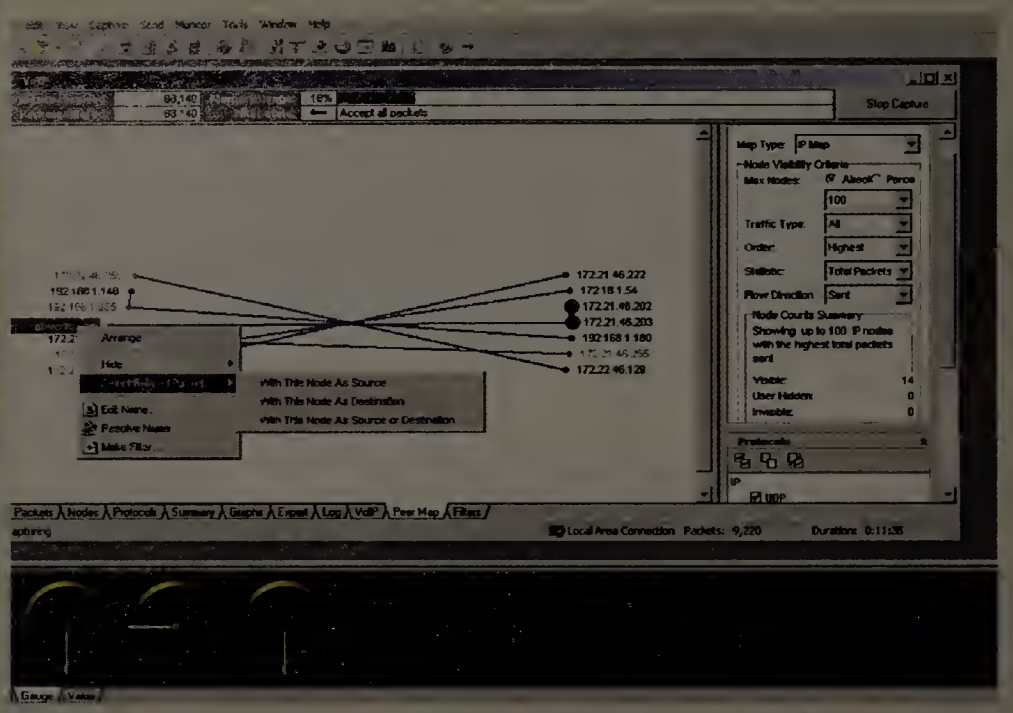


YOU COULD WIN!

A $350 Value!

Go to **www.3com.com/blackberry2005/save1** now to learn more about 3Com switches and enter for your chance to **WIN A BLACKBERRY® HANDHELD!**

3Com
Exercise Choice



The window to WildPackets' EtherPeek VX VoIP Analysis: EtherPeek's interface does a great job distinguishing closed VoIP calls from active ones, which is useful in conducting diagnostics. WildPackets also serves up a peer-mapping feature, which is a dynamic representation of real-time flows and connections.

VoIP

continued from page 50

Clean and legible

It's not enough for a VoIP analysis tool to accurately track the information you seek, it must also let you readily locate the data, and view it in a clear, straightforward manner. In this critical area of usability and navigability, these products varied considerably.

ClearSight placed first. All its VoIP data and measurements come from applets launched from one screen. VoIP streams are shown in a log-type table. The user selects any one and drills down for more detail. The graphics are all clean and very legible. A summary tab shows totals for bandwidth and flows. There's a single click to capture and play back any VoIP stream.

WildPackets was close behind (see graphic, this page). EtherPeek VX's interface does a great job distinguishing closed VoIP calls from active calls, which is useful in conducting diagnostics. It's easy to see who is on the phone in real time. Another WildPackets' plus is a very slick peer map feature, a dynamic, graphical representation of real-time flows and connections.

As long as you are working with either SIP or H. 323 protocol streams, Touchstone's interface is refreshingly simple to navigate. A single, well-organized VoIP screen provides seven tabs for individual applets. Everything is structured on a VoIP call-by-call basis; it is easy to capture, trace, record and delete calls.

Agilent's interface provides volumes of technical details, but finding only the data you want can be tedious. The main VoIP display is somewhat awkward to use, and on-screen help could be more, well, helpful.

Fluke's OptiView system can run in monitor or capture mode, and it's difficult to tell which is running at any time. However, the output is different depending on the mode and we found this a constant nuisance. Like Agilent, the wealth of captured data available to the user is impressive. It's just a little complex to find what you're after. The newer set of VoIP applications — including VoIP Properties, Call and Channel Details — are easier to use and navigate than the older data analyzer base of the system, such as Capture Views, Network Monitoring and Expert Views.

The interface and data displays for Viola's NetAlly — while limited to information collected in its simulated tests — are all clean and clear. Brix's package is focused on generating simulated VoIP streams as part of programmed tests, akin to Viola. The Brix user interface is consistent for the various tests, but it takes time to become familiar with the screen navigation techniques using hyperlinks and various buttons.

Reporting

Besides real-time VoIP monitoring, we set aside some test criteria to address any additional, useful reporting capabilities.

Included in this category is the ability to automatically assess the relative quality of selected VoIP calls. The products report VoIP call quality to varying degrees using a confusing mix of different metrics and scales. These range from widely recognized Mean Opinion Score equivalent ratings, which assign a value from 1 to 5, to new and more esoteric scales including Network R factor, E Model, per ITU G.107, and some proprietary methods.

We didn't intend to test which of these techniques is most accurate or best conveys relative VoIP call quality (see related story on tools for specifically assessing call quality, page 44). What we did do is compare the call quality rating of VoIP calls with no impairments, with similar VoIP calls over a network with fairly major impairments. We found that in most cases, the call quality assessment was reduced, to an appropriate extent, by the added impairments.

All the ratings in this category were close with Brix and ClearSight at the higher end, and with Viola and Fluke at the lower end. Brix offers a number of unique telephony-oriented measurements among its test repertoire, such as post dial delay, which is the elapsed time after you dial, until the destination phone rings. ClearSight's package includes some canned, long-term trend reports, which would be useful in service level agreement-monitoring environments. Agilent's package can generate call detail records (CDR) on VoIP calls that it observes. Touchstone similarly can generate CDRs, while Viola says it can interrogate Cisco CallManager CDR records for VoIP call analysis.

Special features

Several of these products offer unique capabilities that the other portion of our methodology did not address.

ClearSight includes the ability to directly decode VoIP calls traversing Wi-Fi wireless networks. It also offers fairly comprehensive monitoring and analysis of video traffic. The ClearSight software can be set up to issue simulated call setup sequences to a VoIP call controller to monitor its uptime and availability. Brix and Viola also support similar call setup simulation and monitoring features.

WildPackets has a feature that lets the user vary network jitter in the playback of a VoIP call, to see the effect on call quality. Fluke offers the ability to deploy and centrally interrogate multiple distributed probes. And Touchstone has a special utility for analyzing VoIP-based DTMF tones, to aid analysis of interactive voice response systems.

In our overall assessment, we found considerable variety in capability and performance based on the VoIP call-control protocol environment. Until SIP emerges as the ubiquitous VoIP standard — and most agree that's likely over the next two years — users need to correctly mate tools such as these with their particular protocols, IP PBX systems and/or other major VoIP applications.

Edwin Mier is president of Miercom, a network-product test center based in East Windsor, N.J. Dave Mier is manager of lab testing, and Tarpley is senior lab tester at Miercom. They can be reached at ed@miercom.com, dmier@miercom.com or rtarpley@miercom.com, respectively.

NW Lab Alliance

Miercom also is a member of the Network World Lab Alliance, a cooperative of the premier testers in the network industry, each bringing to bear years of practica experience on every test. For more Lab Alliance information, including what it takes to become a partner, go to www.nwfusion.com/alliance.

How We Did It

Over a two-month period, the VoIP analysis tools were connected into our test bed made up of four IP PBX systems, which were:

- EADS Telecom's Nexspan L system, which uses a proprietary, stimulus-based VoIP call-control protocol.
- Mitel Networks' SX-200 ICP, which uses a proprietary message-based protocol called MINET for call control.
- NEC's Univerge 7000, which uses both a proprietary stimulus-based call-control protocol called PROTIMS and also supports Session Initiation Protocol-based endpoints via a separate SIP controller.
- PingTel's SIPxchange, which is based fully and exclusively on standard SIP VoIP call control.

The test bed was configured with two subnets simulating a headquarters and a branch location. The two subnets were interconnected using Cisco routers and Extreme Networks switches. The WAN connection was simulated using a Hurricane IP Network Emulator from PacketStorm Communications. The PacketStorm Emulator let us vary our network environment simulating various impairments including latency, jitter and packet loss.

A mirrored port was configured on the headquarter subnet for the VoIP analysis tools. Five of the seven tools were connected using this port, but the Brix and the Viola products had connections on both sides of our WAN. These two products can generate simulated traffic between their own endpoints to assess the performance of the connecting link.

We used more than eight IP phones to generate real VoIP call traffic between the headquarters and branch subnets. Additionally, some calls were made locally on only the headquarter subnet. Up to four separate VoIP phone calls were placed concurrently, as were conference calls. Before, during and after the calls, the VoIP tools were used to examine the characteristics of the call flows. We used the tools to display call initiation and setup, signaling and any performance statistics relating to the actual VoIP conversation itself.

Nortel's VPN Gateway 3050 is the cost-effective SSL solution for secure remote access.

Nortel's VPN Gateways provide a compelling web-based (SSL VPN) solution for extending secure access to remote/mobile employees, partners and customers. By leveraging SSL-enabled web browsers and by supporting traditional IPsec-based VPN clients, the Nortel VPN Gateway family offers the most convenient, flexible and cost-effective secure remote solutions on the market today.

- Secure anywhere, anytime access for mobile employees, extranets, email and VoIP
- Blended support for both SSL & IPsec VPN access
- Robust remote endpoint security enforcement

NORTEL
Authorized
Distributor

Anytime, anywhere, Westcon is there for you with exceptional training and support.

You've come to expect superior technical expertise and intensive sales support from Westcon, but our commitment to customer care also extends to marketing programs, logistics services and interactive training seminars. Anytime, anywhere, Westcon is there for you.

Up to $5,000 in rebates for purchasing VPN Gateway 3050 or 3070 with multi-user licenses. Visit our website for full details and restrictions.

westcon
networking together®

1-877-779-3342 • www.westcon.com/nortelwebtrack

Smarter Edge | Convergence Edge | Government Edge

Management Strategies

- CAREER DEVELOPMENT
- PROJECT MANAGEMENT
- BUSINESS JUSTIFICATION

New leaders make their mark

CIOs ease transition by getting lay of land before tackling staffing structure and process improvements.

■ BY STACY COWLEY

When an outside leader comes in to run an IT team, the adjustment can be rough — for the current staff and the new executive alike. Several CIOs who have recently made the jump say communication and preparation are critical for ensuring changes are well received.

"I concentrated my first 100 days on doing a lot of listening," says Linda Jojo, who took on the CIO position at Irving, Texas, industrial fluid pumps maker Flowserve in July.

She arrived at a transitional time for the company, which rapidly expanded through mergers into an organization with more than $2 billion in annual revenue. That growth explosion left the company with a patchwork of systems and flawed internal financial controls. Targeted by a Securities and Exchange Commission investigation, Flowserve restated its financial results last year and expects to do so again. It also recently overhauled its management team.

Jojo, who previously spent more than a decade at General Electric and served as CIO of GE Silicones, knew going in about the challenges Flowserve faces and the changes underway. One of her first decisions was to restructure Flowserve's IT organization. She kept the staff size about the same — 250 people scattered throughout more than 50 countries — but aimed to improve internal communication by forming groups of staffers focused on similar tasks such as networking or data center operations. That meant hiring new people, letting some employees go and promoting others.

After spending several months mapping out the skills of Flowserve's employees and determining the most effective way to group them, Jojo announced her new team at the beginning of January. Frequent discussions with staffers and other business unit leaders throughout the organization have been essential, she says.

"There's no question that change management is my biggest time commitment right now," she says. "You have to communicate your message over and over again. Don't assume that if you've said it at one town hall, everyone knows."

"There's no question that change management is my biggest time commitment right now."

Linda Jojo
CIO, Flowserve

Process improvement

Restaurant chain operator Applebee's International in Overland Park, Kan., last year decided to expand the scope of its IT head position and appoint a CIO for the first time. Mike Czinege took the job in April. Before he did, he spent substantial time discussing with Applebee's executives their history with and future plans for IT projects.

"To me, interviewing for this level position is a two-way street," Czinege says. "My interest was, first of all, in understanding what their vision of the business is and what their view of the IT role in that is. We did a lot of soul-searching."

Applebee's top management saw effective IT management as critical to scaling their business, and Czinege says he appreciated that certain key IT decisions made before he joined were astute. Applebee's had just finished a broad PeopleSoft ERP rollout, which was done without major customization.

Czinege says he was happy with the 90-person IT staff Applebee's had in place, so he hasn't had to face the tricky issue of replacing current staff, but he found organizational processes that needed changing. "Within the IT group there were probably more disconnects than I would have expected," he says. "We had a lot of good people doing a lot of good things without a lot of good processes."

He also sees communication skills as the best asset a new leader has in successfully guiding changes.

"You have to have a vision of where you want to go and what's important, and you have to bring people along and get them to buy into that vision. Let them help you craft it," Czinege says. "They had been here a lot longer than I had. They wanted to make changes and improvements as much or more than I did. Once you get everyone aligned on where you're going, their energies and efforts will be the driving force."

"Once you get everyone aligned on where you're going, their energies and efforts will be the driving force."

Mike Czinege
CIO, Applebee's International

Applebee's track record with custom application development work had been spotty, so one of Czinege's first moves was to compile a list of major projects underway and organize "deep dive" meetings for each. Those meetings led to a few projects being put on hold and specific plans being laid for completing the rest.

Czinege says he hopes a more concrete development methodology, with mapped-out processes for steps such as change management and quality-assurance testing, will keep current projects, such as a large point-of-sale system rollout, from getting "lost in the weeds" as past projects had.

Leadership material

Companies are aware that leadership ability is critical, and they'll prioritize "soft skills," such as an aptitude for working well with colleagues, even when hiring for a technical position such as CTO or CIO, according to recruiter Beverly Lieberman. Lieberman is president of executive search firm Halbrecht Lieberman Associates, which specializes in the IT field.

"Usually the top priority is a really strong knowledge of business management, followed by an understanding of the company's industry and competitors, and strong leadership skills," Lieberman says. "Maybe third or fourth on the list is 'it would be great if a candidate has broad technical skills.'"

Czinege, for one, doesn't consider himself a hardcore techie: "I did not come to this job with a deep, deep technical background," he says. "I've been in IS for a long time, but more from a consulting perspective — process reengineering and implementing applications."

Soft skills are so critical that Lieberman estimates 20% of Fortune 500-size businesses have some form of psychological testing as part of their interview process for top IT executives. The goal is to make sure a new executive can guide their subordinates as successfully as they can steer a new ERP deployment.

Lieberman advises candidates to be frank — at least, once they've reached the finalist stage — with potential employers about their needs and concerns about taking on a leadership role over a current IT team.

"Once you know you're kind of the person they want to hire, that discussion is important," she says. "Especially if it's a step up. If someone is used to managing a staff of 100 and now they'll be managing a staff of 500, there's some need for learning and validation. I'll say to the client, 'We are aware that this might be a stretch job for this person. What resources, what coaching, what training can you provide?'"

Czinege and Jojo say a key aspect of their recruiting process was their evaluation of their potential new employers and the top management's commitment to IT.

"The first part is understanding what's there," Czinege says. "You want to make sure that's who you want to get on the bus with."

Cowley is a correspondent with the IDG News Service.

HIT SPYWARE. HARD.

Your weapon: CounterSpy Enterprise. Centralized spyware eradication.

Spyware: the new number one enemy for IT. Recent surveys of IT specialists show that spyware infections have reached epidemic proportions. Spyware is one of the most serious security threats and productivity killers today. It's insidious. Its creators are well-financed, relentless and remorseless. For the enterprise, common antispyware can't cut it.

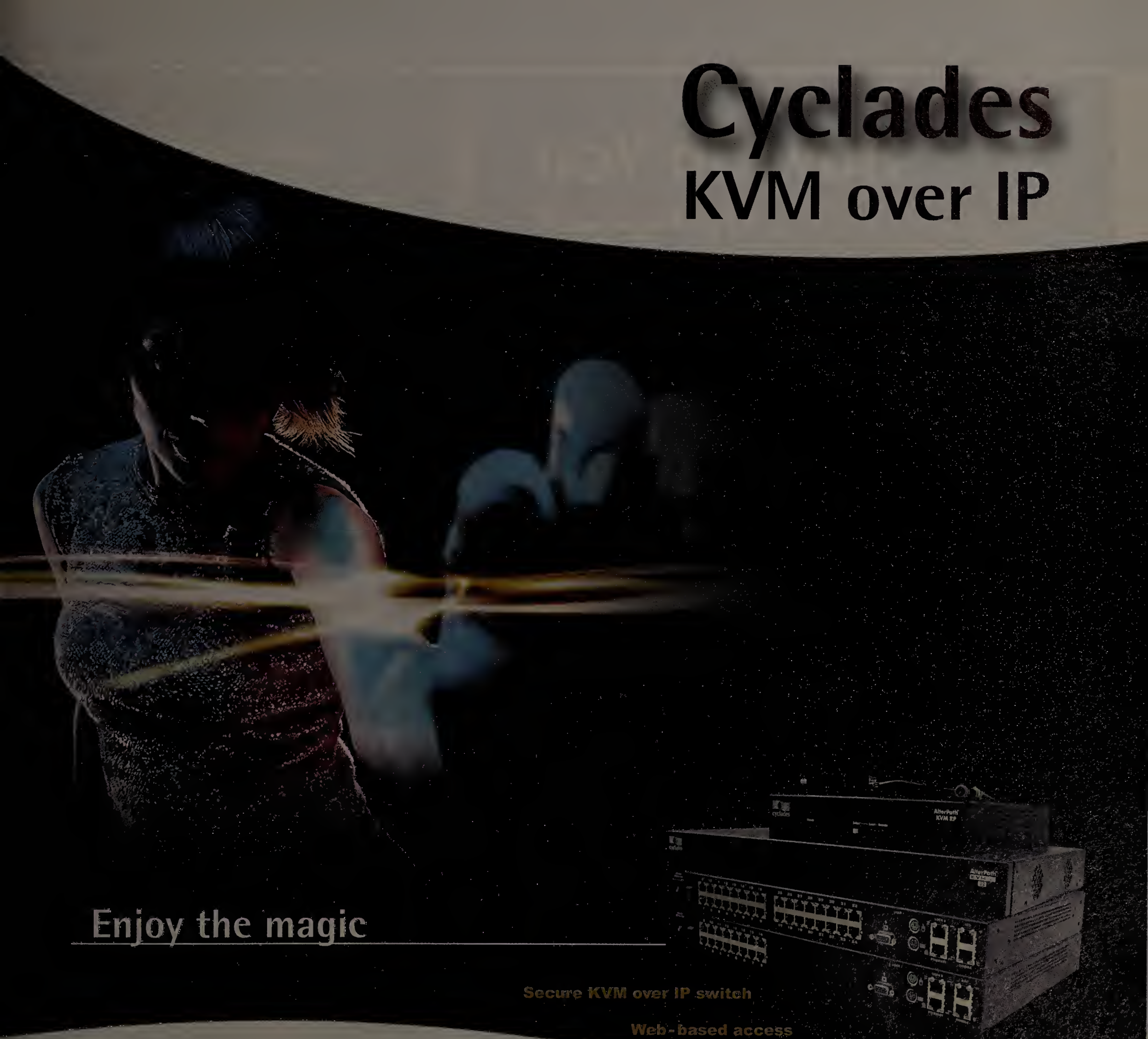
CounterSpy Enterprise: Knock out spyware from one centralized location. Company-wide spyware management requires a real enterprise product with *centralized* management. CounterSpy Enterprise is just that: a scalable, policy-based, second-generation antispyware tool built from the ground up by and for system- and network administrators to kill spyware quickly and easily.

Powerful, comprehensive spyware scanning. CounterSpy's scanning engine uses threat signatures from multiple sources to hunt down and delete more than 30 categories of spyware, adware, and other malware. Spyware doesn't stand a chance. **We've recruited an army to combat spyware.** New spyware comes out all the time. That's why, in addition to our own research team, we have CounterSpy ThreatNet.™ Customers of our consumer version report new potential threats to ThreatNet for analysis. Then we propagate new threat signatures to all users—consumer and enterprise. Sunbelt combines forces to hit spyware. Hard. **Free trial. Find out how many machines in your organization are infected.** Scan your machines for free. Get it here: *www.sunbelt-software.com/csenww.*

SUNBELT SOFTWARE

Sunbelt Software Tel: 1-888-NTUTILS (688-8457) or 1-727-562-0101 Fax: 1-727-562-5199 www.sunbelt-software.com sales@sunbelt-software.com

Cyclades
KVM over IP



Enjoy the magic

Secure KVM over IP switch

Web-based access

Centralized system management

Remote incident resolution

Cyclades AlterPath™ KVM/net offers a unique set of features:

- Server-based authentication
  (NT domain, LDAP, Secure ID, RADIUS, TACACS+)
- 16 and 32 port models
- CAT5 cabling up to 500 feet
- User access logging
- System event syslog
- Integrated power management

We've worked our magic.
Now you can work yours.

Over 85% of Fortune 100 choose Cyclades.

www.cyclades.com/nw

1.888.cyclades · sales@cyclades.com

cyclades

Anti-spam technology failing? Well...

YOU'VE BEEN SCAMMED!

Meridius Security Gateway™

99% spam detection rate,
0% false positives,
100% virus blocking†

Call 1.866.895.6931 and get a $5000* trade-in credit

* Contact a BlueCat Networks representative for promotion details. Limited time offer. Promotion code: BCN-M105
† "Scanning for Spam", Network Computing Magazine Oct. 28, 2004

INSIDE·THE·DOMAIN™
www.bluecatnetworks.com/subscribe

BlueCat Networks
secure networks. simplified.

Call us:
1.866.895.6931

Schedule your free demo today.
Visit www.bluecatnetworks.com/meridius/nww

Meridius Security Gateway™

NetworkWorld

Editorial Index

Advertiser Index

Network World Fusion - www.nwfusion.com

3Com	Network Associates
ADIC	Nokia
Airespace	Nortel Networks
Allot Communications	Oracle Corporation
Avaya	PatchLink Corporation
BMC	Program Deliverables
Broadcom Corporation	Qwest Communications
CDW	RADWARE
Ceonex, Inc.	Redline Networks
Chantry Networks	Remedy
Cisco Systems, Inc.	Riverbed Technology
Computer Associates	RSA Security Inc.
DuPont	SBC
EMC Corp	Schmidt's LOGIN GmbH
Engenio	Sprint
Finisar Corp	SSH Communications
Groundwork	Statscout Pty Ltd
HP	Texas Instruments
IBM	Trend Micro
Imprivata	TrendsMedia Inc.
Intel Corporation	Tripp Lite
IronPort Systems	VeriSign Inc
Juniper Networks Inc	Verizon Wireless Broadband
Lucent Technologies	Webroot
Meru	Xerox
Microsoft Corporation	

These indexes are provided as a reader service. Although every effort has been made to make them as complete as possible, the publisher does not assume liability for errors or omissions.

*Indicates Regional Demographic

Network World, Inc.

118 Turnpike Road, Southborough, MA 01772
Phone: (508) 460-3333

TO SEND E-MAIL TO NWW STAFF
firstname_lastname@nww.com

Evilee Thibeault, CEO/Publisher
John Gallant, President/Editorial Director
W. Michael Draper, Chief Operating Officer
Eleni Brisbois, Administrative Planning Manager

FINANCE
Mary Fanning, Vice President Finance
Paul Mercer, Finance Manager
Betty Amaro-White, Event Finance Manager

HUMAN RESOURCES
Eric Cormier, Sr. Human Resources Generalist

MARKETING
TerryAnn Croci, Sr. Director of Customer Experience
Nancy Sarian, Corporate Marketing Communications Mgr.
Barbara Sullivan, Senior Research Analyst
Judy Schultz, Marketing Design Manager
Cindy Panzera, Marketing Designer

PRODUCTION SERVICES
Greg Morgan, Senior Director, Production Services
Karen Wallace, Senior Director, Advertising Operations
Mike Guerin, Manager of Production Technologies
Jami Thompson, Sr. Production Coordinator
Veronica Trotto, Online Operations Coordinator
Jane Wilbur, Online Ad Traffic Coordinator
Mare Eremyan, Advertising Coordinator
Christina Pankievich, Advertising Coordinator

CIRCULATION
Richard Friante, Senior Director of Circulation
Bobbie Cruse, Subscriptions Manager
Mary McIntire, Sr. Circulation Marketing Manager

RESEARCH
Ann MacKay, Research Director

DISTRIBUTION
Bob Wescott, Distribution Manager/(508) 879-0700

IDG LIST RENTAL SERVICES
Amy Bonner, Account Executive
P.O. Box 9151, Framingham, MA 01701-9151
Toll free: (800) 434-5478 ext. 6026/Direct:(508) 370-0826
Fax: (508) 370-0020

SEMINARS, EVENTS AND IDG EXECUTIVE FORUMS
Neal Silverman, Vice President of Events & E. F.
Mike Garity, Director of Business Development
Michele Zarella, Director of Operations
Dale Fisher, Senior Event Planner
Jacqueline DiPerna, Event Coordinator
Karen Bornstein, Sales Operations Specialist
Danielle Bourke, Event Operations Coordinator
Andrea D'Amato, National Sales Director Events
Kristin Ballou-Cianci, Event Regional Account Director
Jennifer Sand, Regional Account Manager
Cedric Fellows, Regional Account Manager
Mark Hollister, Senior Director of Event Marketing
Debra Becker, Dir., Marketing & Audience Development
Sara Nieburg, Senior Marketing Manager
Dori Smith, Event Database Manager
Buster Paris, Marketing Specialist

ONLINE SERVICES
Kevin Normandeau, Vice President, Online
Dan Gallagher, Director of Audience Development, Online
Norm Olean, Director of Business Development, Online
Adam Gaffin, Executive Editor, Online
Melissa Shaw, Managing Editor, Online
Jason Meserve, Multimedia Editor
Sheryl Hodge, Sr. Online Copy Chief
Deborah Vozikis, Design Manager Online

CLIENT SERVICES
W. Michael Draper, Chief Operating Officer
Sharon Stearns, Director of Client Services
Leigh Gagin, Client Services Manager
Kristin Miles, Client Services Specialist

INFORMATION SYSTEMS/BUSINESS SERVICES
W. Michael Draper, Chief Operating Officer
Tom Kroon, Director of Systems Development
Anne Nickinello, Senior Systems Analyst
Puneet Narang, Manager of Database Technologies
William Zhang, Senior Software Engineer
Manav Seghal, Senior Software Engineer
Rocco Bortone, Director of Network IT
Peter Hebenstreit, Senior Network/Telecom Engineer
Brian Wood, Senior Systems Support Specialist
Frank Coelho, Senior Manager, Business Services
Mark Anderson, Business Services Supervisor
Linda Cavanagh, Business Services Administrator

IDG

Patrick J. McGovern, Chairman of the Board
Pat Kenealy, CEO

Network World is a publication of IDG, the world's largest publisher of computer-related information and the leading global provider of information services on information technology. IDG publishes over 275 computer publications in 75 countries. Ninety million people read one or more IDG publications each month. *Network World* contributes to the IDG News Service, offering the latest on domestic and international computer news.

Sales Offices

Carol Lasker, Associate Publisher/Vice President
Jane Weissman, Sales Operations Manager
Internet: clasker, jweissman@nww.com
(508) 460-3333/FAX: (508) 460-1237

New York/New Jersey
Tom Davis, Associate Publisher, Eastern Region
Elisa Della Rocco, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: tdavis, elisas, ajoseph@nww.com
(201) 634-2300/FAX: (201) 634-9286

Northeast
Elisa Della Rocco, Regional Account Director
Internet: elisas@nww.com
(508) 460-3333/FAX: (508) 460-1237

Mid-Atlantic
Jacqui DiBianca, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: jdibian, ajoseph@nww.com
(610) 971-1530/FAX: (610) 975-0837

Midwest/Central
Eric Danetz, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: edanetz, ajoseph@nww.com
(201) 634-2314/FAX: (201) 712-9786

Southeast
Don Seay, Regional Account Director
Agata Joseph, Senior Sales Associate
Internet: dseay, ajoseph@nww.com
(404) 504-6225/FAX: (404) 504-6212

Northern California/Northwest
Sandra Kupiec, Associate Publisher, Western Region
Karen Wilde, Regional Account Director
Courtney Cochrane, Regional Account Director
Vanessa Tormey, Regional Account Manager
Teri Marsh, Sales Assistant
Jennifer Hallett, Sales Assistant
Internet: skupiec, kwilde, ccochrane, vtormey, tmarsh, jhallett@nww.com
(510) 768-2800/FAX: (510) 768-2801

Southwest/Rockies
Becky Bogart Randell, Regional Account Director
Internet: brandell@nww.com
(949) 250-3006/FAX: (949) 833-2857

Online/Integrated Solutions
Kevin Normandeau, Vice President, Online
Susan Cardoza, National Sales Director, Integrated Solutions
Scott Buckler, Director of Integrated Solutions
Stephanie Gutierrez, Online Acct. Manager, Integrated Solutions
Michael Hiatt, Director of Integrated Solutions
James Kalbach, Director of Integrated Solutions
Debbie Lovell, Online Account Manager, Integrated Solutions
Kate Zinn, Director of Integrated Solutions
Denise Landry, Sales Coordinator
Lisa Thompson, Sales Coordinator
Internet: knormandeau, scardoza, sbuckler, sgutierrez, mhiatt, jkalbach, dlovell, kzinn, dlandry, lthompson@nww.com
(508) 460-3333/FAX: (508) 861-0467

MARKETPLACE/EMERGING MARKETS
Donna Pomponi, Director of Emerging Markets
Enku Gubaie, Manager of Marketplace/Emerging Markets
Caitlin Horgan, Manager of Marketplace/Emerging Markets
Jennifer Moberg, Manager of Marketplace/Emerging Markets
Chris Gibney, Sales Operations Coordinator
Internet: dpomponi, egubaie, chorgen, jmoberg, cgibney@nww.com
(508) 460-3333/FAX: (508) 460-1192

April Fool's
continued from page 1

which issues a phony computer network RFC every year. The RFC Editor, the publisher of Internet standards and best practices, has been publishing April 1 RFCs since 1983.

Every year, network engineers worldwide await the release of the latest April Fool's Day RFC. These documents feature satire that would make Jonathan Swift proud (if he could understand the technical references).

"The best April Fool's Day RFCs reveal truth by telling a lie," Bradner writes in the introduction of a soon-to-be-published archive of April 1 RFCs. These RFCs "play it straight but describe something that could not or should not be done."

Bradner has authored or coauthored three April 1 RFCs and been the butt of another. "There were other attempts that did not see the light of day and probably should not have," he quips.

The trick in writing a good April 1 RFC is to make it look and sound real. Many of these documents have fooled network engineers into trying to implement them.

"I take pride in the fact that about half of the many comments I received about each of the last two April 1st RFCs I've been involved in thought that I was serious," Bradner says. The Omniscience Protocol "even got Slashdotted."

The story behind April Fool's Day

The tradition of playing pranks on April 1 dates back to 1564, when the French officially changed their calendars to move New Year's Day from April 1 to Jan. 1. People who hadn't heard of the change and still celebrated New Year's Day on April 1 were considered fools.

The RFC Editor started its April Fool's Day tradition more than 20 years ago, when Internet pioneer Jon Postel was in charge of standards publication. Since Postel's death in 1998, the RFC Editor shop at the University of Southern California's Information Sciences Institute has carried on the beloved tradition.

The RFC Editor solicits submissions for April 1 RFCs from the IETF, which is the Internet's premier standards-setting body. Submissions are accepted until mid-March, then the six-person RFC Editor team reads them and decides which is funniest.

"It has to be something technical that you want to believe in," says Joyce Reynolds, Internet Services Manager for the RFC Editor. "It has to be written in a very tongue-in-cheek manner."

The format of April 1 RFCs is the same as regular RFCs, and publication is announced by the IETF just like any other RFC. The only clue to readers that the document is a joke is the publication date of April 1. Regular RFCs list only the month of publication.

Some years, the RFC Editor team publishes many April 1 RFCs. In the last 20-plus years, the group has never run into the situation where they didn't have a submission humorous enough to publish.

"The fun part about it is that everyone in the IETF waits to see what we're going to publish," Reynolds says. "We know they're popular by the number of hits we get on our Web site."

The April 1 RFCs remain permanently in the official archives of the RFC Editor. Sometimes network engineers think they are real documents and try to prototype them.

"We'll get e-mail saying that someone is having trouble implementing an April 1 RFC," Reynolds says. "The e-mail could come years later."

Two of the most famous April 1 RFCs were written in the 1990s by David Waitzman, a senior software engineer with BBN Technologies who says each of the documents took less than a day to write.

In RFC 1149, Waitzman describes a technique for how IP packets can be transmitted via pigeon carriers.

"The IP datagram is printed on a small scroll of paper in hexadecimal ... [and] wrapped around one leg of the avian carrier," Waitzman writes. "Upon receipt, the duct tape is removed and the paper copy of the datagram is optically scanned into a electronically transmittable form."

"RFC 1149 is very popular in the technical community," says Bob Braden, who serves as RFC Editor. "There are many references to the avian carriers document in other publications."

The Bergen Linux User Group in Norway actually implemented this RFC in 2001 (see www.nwfusion.com, DocFinder: 6436). A reference to RFC 1149 also was slipped into Cisco product literature as a joke by an IETF leader.

Waitzman followed up in 1999 with RFC 2549 entitled "IP Over Avian Carriers with Quality of Service." This document discusses the pros and cons of having ostriches, robins, hawks, penguins and other birds serve as carriers of IP packets. "There are privacy issues with stool pigeons," Waitzman jokes.

The April Fool's Day RFC tradition "reflects the classic IETF attitude of not taking itself too seriously," Waitzman writes via e-mail.

"You'd never see the ISO or IEEE organizations do humor (which they would argue is exactly as it should be)," he writes.

Braden says the best April Fool's Day RFCs are original, describe something technically relevant and feature clever writing.

"Good satire is hard to write," he says. "People tend to be heavy-handed. Subtlety is really good. You want to laugh out loud the first time you read it."

Braden's favorite is RFC 3514, which was written by security expert Steve Bellovin, a professor of computer science at Columbia University.

Bellovin's RFC describes the creation of an "evil bit" in the header of messages that mean to do harm such as spam, viruses, denial-of-service attacks and other malicious traffic. This evil bit would let firewalls, filters and intrusion-detection systems identify and block packets with malicious intent.

Bellovin says he wrote the evil bit document on a cross-country plane ride. "I'd been using the phrase for years when speaking about firewalls and network security," Bellovin says. "I finally thought of it at the right time of the year."

Publishing an April 1 RFC is a tradition that members of the IETF community look forward to every year.

"There's a lot of anticipation" of the April 1 RFCs, says Patrik Faltstrom, a Cisco engineer and member of the Internet Architecture Board. Faltstrom submitted one April Fool's Day RFC, but it wasn't published. "Why spend energy on this? Because you need to have fun." ■

Got great ideas

■ Got a suggestion for a Wider Net story? An offbeat network industry-related topic? A fascinating personality we should profile? Contact Bob Brown with your ideas at bbrown@nww.com.

More online!

Read a sampling of April Fool's Day RFCs from the Internet engineering community.

DocFinder: 6460

Cupps
continued from page 15

many ways.

How does your company handle software patching?

We use the Windows system for our desktops and Tivoli, Altiris or manual patching for the servers. We are increasingly relying on host-based IPS and Determina memory firewalls to help cover the gap times.

You've adopted intrusion-prevention technology. Why, and how much of an issue are false positives these days?

For the McAfee stuff I am getting some, but it is manageable. Most of it is coming from the firewall portion, and to be honest, I can't blame it on the [McAfee] Entercept piece. For the Determina stuff I haven't seen any false positives yet.

You've mentioned Determina a couple of times. What's your general take on buying from start-ups?

I don't have a problem buying from start-ups. First, you have to test any product you buy thoroughly, regardless of what it is to ensure it works in the way you want it within your environment. You can have a product failure from the largest, most established companies, as well as the smaller ones.

Second, most tech purchases now last only a few years anyway, whether they are [operating systems] or apps. There seems to be a two- to three-year cycle, and most upgrades require a lot of rework and learning even within a single named app.

Third, there are often price benefits, both initially and with total cost of ownership, when dealing with more aggressive companies. I have found service and support to be much more favorable in many smaller companies. ■

■ **Network World**, 118 Turnpike Road, Southborough, MA 01772-9108. (508) 460-3333.

Periodicals postage paid at Southborough, Mass., and additional mailing offices. Posted under Canadian International Publication agreement #40063800. Network World (ISSN 0887-7661) is published weekly, except for a single combined issue for the last week in December and the first week in January by Network World, Inc., 118 Turnpike Road, Southborough, MA 01772-9108.

Network World is distributed free of charge in the U.S. to qualified management or professionals.

To apply for a free subscription, go to www.subscribenw.com or write Network World at the address below. No subscriptions accepted without complete identification of subscriber's name, job function, company or organization. Based on the information supplied, the publisher reserves the right to reject non-qualified requests. Subscriptions: 1-508-490-6444.

Nonqualified subscribers: $5.00 a copy; U.S. - $129 a year; Canada - $160.50 (including 7% GST, GST#126659952); Central & South America - $150 a year (surface mail); Europe - $205 a year (surface mail), all other countries - $300 a year (airmail service). Four weeks notice is required for change of address. Allow six weeks for new subscription service to begin. Please include mailing label from front cover of the publication.

Network World can be purchased on 35mm microfilm through University Microfilm Int., Periodical Entry Dept., 300 Zebb Road, Ann Arbor, Mich. 48106.

POSTMASTER: Send Change of Address to **Network World**, P.O. Box 3090, Northbrook, IL 60065. Canadian Postmaster: Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A7C9.

BPA INTERNATIONAL

Copyright 2004 by Network World, Inc. All rights reserved. Reproduction of material appearing in Network World is forbidden without written permission.

Reprints (minimum 500 copies) and permission to reprint may be purchased from Reprint Management Services at (717) 399-1900 x124 or rtry@rmsreprints.com.

USPS735-730

STAND UP AND BE COUNTED

Enter today at
www.nwfusion.com/renovator2005.html

DocFinder: 5951

Enter the

NetworkWorld® Renovator Award

program

Have you overhauled your network and realized a substantial ROI, discovered a significant new business opportunity or found a creative way to leverage technology?

If so, get in the running for *Network World's* new **Renovator Award,** the top winners of which will be honored at a celebration in Las Vegas during the NetWorld+Interop conference, May 3-5.

Entries will be judged by a panel of *Network World* editors, columnists and industry experts. Winners will be presented an award at the celebration and profiled in a subsequent *Network World* story.

JUDGING PANEL

Bob Brown
Executive News Editor, *Network World*

John Dix
Editor in Chief, *Network World*

Lee Doyle
Group VP, Network Infrastructure, IDC

Daniel Golding
Senior Analyst, Burton Group

Johna Till Johnson
Founder and CRO at Nemertes Research

Jeff Wilson
Principal Analyst, Infonetics

Robert Whiteley
Analyst, Forrester Research

sponsored by Juniper® NETWORKS

BackSpin Mark Gibbs

The need (or not) for data havens

Did you read *Network World's* Wider Net article a few weeks ago, "Selling bunker mentality to IT shops"? The story concerns a slightly eccentric couple, Don and Charlene Zwonitzer, who purchased a 1960s-era Atlas E Missile Silo and converted it "into home sweet home — and eventually, they hope, a modern-day computer disaster-recovery facility."

The idea makes a lot of sense. This building is 20,000 square feet, has 2-foot-thick walls and ceilings constructed from 139,000 cubic yards of reinforced concrete and 27,840 tons of structural steel, and can withstand a 1-megaton blast up to 1.6 miles away. Sounds really cozy and for a disaster-recovery facility, highly sensible.

Not that setting up such a service is easy. A company called Underground Secure Data Center Operations (USDCO) opened its subterranean doors in July 2001 in a disused gypsum mine near Grand Rapids, Mich. It seems local zoning laws subsequently conspired to shut down the company sometime in 2003. Curiously, despite a lot of positive press when USDCO opened (www.nwfusion.com, DocFinder: 6461), its passing was barely noticed.

Of course, we're talking about facilities on U.S. soil. While they might be disaster-proof, they wouldn't meet the criteria for organizations that would like both disaster resistance and real privacy.

For that kind of service, you'll have to go to somewhere like Sealand. Sealand is a reclaimed World War II British artificial island fortress a few miles off the English coast. With a surface area roughly equal to that of a basketball court, Sealand is a real country complete with passports, stamps and all the trappings of sovereignty.

Sealand's history is an extraordinary story of brave, but loosely wrapped people. Roy Bates, the "crown prince" of Sealand, sailed out to the platform in 1966 and claimed it as an independent nation. The British government wasn't too keen on this and tried to kick the Bates Royal Family off the platform, but the law, it turns out, was on the side of Crown Prince Roy.

Sealand's independence was upheld in a 1968 British court decision on the grounds that the structure, called Rough's Tower, was in international waters and thus did not fall under the legal jurisdiction of the U.K. According the official Sealand home page (www.sealandgov.com), this judgment "gave birth to Sealand's national motto of 'E Mare Libertas,' or 'From the Sea, Freedom.'"

It is from this platform that HavenCo, a data warehousing operation registered in Anguilla, operates. HavenCo boasts "Unsurpassed physical security from the world" and immunity from "government subpoenas [as well as] search and seizures of equipment and data."

So if you want to store your data somewhere that's potentially as physically and legally secure as can be, then it looks like HavenCo might be the place.

HavenCo says: "Sealand currently has no regulations regarding copyright, patents, libel, restrictions on political speech, non-disclosure agreements, cryptography, restrictions on maintaining customer records, tax or mandatory licensing, [Digital Millennium Copyright Act], music sharing services, or other issues; child pornography is the only content explicitly prohibited." HavenCo also prohibits spamming.

So running non-regulated gambling operations, money laundering, and all sorts of interesting activities could be legally, by Sealand's laws, going on.

This raises interesting issues for Sealand and HavenCo should any major governments take objection to what HavenCo's customers might be up to. I'm wondering to what extent should Sealand's, and therefore HavenCo's, rights be protected?

Does the world need safe data havens? Is it consistent with our need for increased security in the face of terrorism that such places should exist, or is our commitment to democracy so profound that we recognize Sealand's sovereignty?

Let's hear your opinion at backspin@gibbs.com.

Layer 8 A coffee break for your head

By Melissa Shaw

Microsoft knows why you're happy

If you're happy at work, Microsoft says you can thank your reliable mouse and keyboard!

So sayeth a hilarious press release from Redmond:

"Reliable Mice and Keyboards Boost Workplace Morale: New Survey Suggests Happiness and Productivity Linked to High-Quality Technology."

Here's the intro: "If it feels like you are more productive at work than ever, take heart; it's probably true. According to a new survey commissioned by Microsoft Hardware, that increased productivity is brought to you by a close relationship with your computer."

Further down: "In addition, when asked to rate a selection of mice and keyboard manufacturers, Microsoft was the company respondents most associated with reliable, high-quality hardware peripherals."

Well, now we can throw away our Prozac.

www.nwfusion.com, **DocFinder: 6442**

Crazy 'Net buy of the week

We thought *The New York Times'* $410 million purchase of About.com in February was, frankly, nuts. Well, media mogul Barry Diller sees that and raises.

The tech world last week was all atwitter with the news Diller's Internet arm, IAC/InterActiveCorp, has offered to buy search engine Ask Jeeves for $1.85 billion. As we wrote with the About.com news, "we sincerely hope that [figure is] in pesos or magic beans."

Other IAC sites include Expedia, Citysearch, Match.com and Evite. We are so in the wrong business.

Actually, now that we think about it, this acquisition kinda makes sense. We forgot Diller created Fox. **DocFinder: 6443**

Ireland: The high cost of broadband

If you go to the Emerald Isle, two things are very expensive: Irish-knit sweaters and broadband.

The Register reports that Ireland is the fourth most expensive place to get broadband in the world, topped only by Luxembourg, Denmark and Iceland.

The site says residents can expect to pay 39.99 Euros a month (about $52) for a 512K connection. If you want the best bargain, head to Korea, where you'll pay 13 Euros ($17) for a 2.5M connection. **DocFinder: 6444**

E-mail aliens, waste money

For only $19.95 you can now spam aliens.

Those who visit www.TalkToAliens.com and pony up the dough can write a message of up to 1,000 words. The e-mail is then broadcast into deep space. You'll even get a souvenir: A "Certificate of Interstellar Broadcast" — "a frameable certificate that indicates the date and time of the broadcast, as well as the first 500 characters of the message sent."

We smell a new acquisition target for Barry Diller. **DocFinder: 6445**

Inside 'Free iPod' deals

They pop up over and under your browser and into your in-box — come-ons offering you a "FREE IPOD!!!"

Now you and I know it's most likely a scam, and so suspected San Francisco columnist David Lazarus, who actually investigated one such offer.

Not surprising, Lazarus found that to get the iPod, you have to wade through reams of surveys and marketing offers, and also provide personal information. What was surprising was that the company behind the offer has partnered with large, legit businesses such as AOL, Blockbuster, Citibank, EarthLink, General Motors and *USA Today*. **DocFinder: 6446**

Shaw is managing editor of www.nwfusion.com, the online component of Network World. *She can be reached at mshaw@nww.com.*

The right technology (at the right price).

ADTRAN PoE 802.3af Power over Ethernet

NetVanta 1224R/1224STR Series
Network-in-a-Box with
Switch/Router/Firewall/VPN/DSU/CSU

New!

NetVanta 1224/1224ST Series
Managed Fast Ethernet and
Powered Ethernet Switches

NetVanta 1524ST
Managed Gigabit Ethernet Switch

NetVanta 340
Business-class ADSL2+ Router

NetVanta 3200
Modular 2xT1/ADSL2+ Branch Office
Routers with Firewall/VPN/Voice/Dial Backup

NetVanta 3205/3305/4305
Modular 2xT1/3xT1/8xT1 Routers with
Firewall/VPN/Voice/Dial Backup

NetVanta 5305
Modular 2xT3 Router with Firewall/VPN

NetVanta 2050/2054/2100
Home Office/Small Office VPN Gateways
with Firewall/Multi-Port Switch

NetVanta 2300/2400
Medium to Large Office VPN
Gateways with Firewall

NetVanta® Switches, Routers, and VPN Solutions.

Is voice and data networking costing you more than it should? You no longer have to pay premium prices for brand name gear to perform customary internetworking tasks. With the ***NetVanta Series*** from ADTRAN®, you can implement the ***exact internetworking functionality*** you need, at a cost that's often ***50% less*** than competing brand name solutions. Choose from ***switching, routing, and VPN*** platforms. Modular chassis and ***deep product lines*** let you pick and choose just the right solution for ***any application***—data, voice, ***VoIP, Internet***, backup, and management—across networks ranging from 56 kbps to GigE. Every solution is backed by a ***100% satisfaction guarantee*** from ADTRAN, unlimited telephone technical support (before and after the sale), ***free firmware upgrades***, and a full 5-year warranty.

Lower network costs without compromising quality, performance, or support — with NetVanta.

VoIP Ready

Why pay more (when you don't have to)?

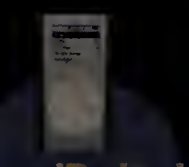
Compare now! Receive a free white paper on reducing total cost of ownership.
www.adtran.com/rightprice

Have a question about network design? How to implement VoIP in your network? Our network engineers are standing by.

800 597 9602 Technical Questions
877 280 8416 Where to Buy

TOLLY Up to Spec CERTIFIED

ADTRAN 5 year Warranty



Win an iPod mini!
N+I
Booth 2324

The Network Access Company ADTRAN®

COLOR SENSE

For just pennies a page, the versatile Xerox WorkCentre® Pro 2128 delivers rich 1200 x 1200 dpi color prints, plus advanced multi-function performance. Xerox Color. It makes business sense.

The remarkable Xerox WorkCentre Pro 2128 gives you an affordable way to add brilliant color and an impressive set of valuable features to any office. This advanced digital system can print, copy, scan, e-mail or fax simultaneously, even when other jobs are running. It also scans hard copy directly to e-mail, improving productivity. Walk-up simplicity means easy access to razor sharp 28 ppm black-and-white and 21 ppm quality color documents. And it consolidates all these functions without compromising reliability. To learn more, see our full line of multi-function systems, digital copiers and award-winning color printers. It makes perfect sense for any business.

Print Copy Scan Fax E-mail

Xerox WorkCentre Pro 2128

XEROX®

xerox.com/office/24
1-800-ASK-XEROX ext. 24

Technology | Document Management | Consulting Services

EVENT PRODUCER

NetworkWorld®

EVENT HOST

Lucent Technologies
Bell Labs Innovations

Creating value through true services convergence™

Johna Till Johnson

John Poole

Join Lucent Technologies, along with our strategic partners Enterasys, Shared Technologies and Sun Microsystems, for ***Creating value through true services convergence™***, a free half-day seminar that will equip you with best practices, tools and technologies for a successful convergence rollout.

Led by Nemertes Research Founder and President **Johna Till Johnson** and Lucent Enterprise Solutions Architect **John Poole**, this educational forum will cover:

- The importance of determining the network's current capacity and ability to handle new traffic.
- How to measure the current quality of service for appropriately handling voice, video, and various types of data traffic.
- How to monitor the performance of the above applications and troubleshoot problems.
- The top three challenges in managing converged service delivery and how Lucent's carrier class can overcome them with ease.
- How convergence can increase productivity.
- Convergence and advanced multimedia applications.
- Converged services across a fixed and wireless infrastructure.
- Using convergence to create the virtual workplace — and why it matters.

COMING TO A CITY NEAR YOU!

- **DALLAS, TX** APRIL 12, 2005
- **SAN JOSE, CA** APRIL 14, 2005
- **NEW YORK, NY** APRIL 26, 2005
- **BOSTON, MA** APRIL 28, 2005
- **WASHINGTON, DC** MAY 10, 2005
- **DENVER, CO** MAY 12, 2005

As a special thank-you from Lucent, all attendees will receive a USB Flash Drive!

To register for this free educational forum, RSVP at **www.nwfusion.com/LS5A or call 1-800-643-4668.**

This event is created for network and IT professionals involved in the planning and purchase of network convergence products and services. Network World Events reviews all registrations and determines total audience profile of complimentary attendees. Incentive to attend does not apply to government employees. "Creating value through true services convergence" is a trademark of Lucent Technologies.

EVENT PARTNERS

enterasys Networks that Know

SHARED TECHNOLOGIES

Sun microsystems

COLOR SENSE

For just pennies a page, the versatile Xerox WorkCentre® Pro 2128 delivers rich 1200 x 1200 dpi color prints, plus advanced multi-function performance. Xerox Color. It makes business sense.

The remarkable Xerox WorkCentre Pro 2128 gives you an affordable way to add brilliant color and an impressive set of valuable features to any office. This advanced digital system can print, copy, scan, e-mail or fax simultaneously, even when other jobs are running. It also scans hard copy directly to e-mail, improving productivity. Walk-up simplicity means easy access to razor sharp 28 ppm black-and-white and 21 ppm quality color documents. And it consolidates all these functions without compromising reliability. To learn more, see our full line of multi-function systems, digital copiers and award-winning color printers. It makes perfect sense for any business.

Print Copy Scan Fax E-mail

Xerox WorkCentre Pro 2128

XEROX®

xerox.com/office/24
1-800-ASK-XEROX ext. 24

Technology | Document Management | Consulting Services